ICSNC 2012

The Seventh International Conference on Systems and Networks Communications

ISBN: 978-1-61208-231-8

November 18-23, 2012

Lisbon, Portugal

ICSNC 2012 Editors

Eugen Borcoci, University Politehnica of Bucarest, Romania

Sathiamoorthy Manoharan, University of Auckland, New Zealand

ICSNC 2012

Forward

The Seventh International Conference on Systems and Networks Communications (ICSNC 2012), held on November 18-23, 2012 in Lisbon, Portugal, continued a series of events covering a broad spectrum of systems and networks related topics.

As a multi-track event, ICSNC 2012 served as a forum for researchers from the academia and the industry, professionals, standard developers, policy makers and practitioners to exchange ideas. The conference covered fundamentals on wireless, high-speed, mobile and Ad hoc networks, security, policy based systems and education systems. Topics targeted design, implementation, testing, use cases, tools, and lessons learnt for such networks and systems

The conference had the following tracks:

- WINET: Wireless networks
- HSNET: High speed networks
- SENET: Sensor networks
- MHNET: Mobile and Ad hoc networks
- VENET: Vehicular networks
- RFID: Radio-frequency identification systems
- SESYS: Security systems
- MCSYS: Multimedia communications systems
- POSYS: Policy-based systems
- PESYS: Pervasive education system

We welcomed technical papers presenting research and practical results, position papers addressing the pros and cons of specific proposals, such as those being discussed in the standard forums or in industry consortiums, survey papers addressing the key problems and solutions on any of the above topics, short papers on work in progress, and panel proposals.

We take here the opportunity to warmly thank all the members of the ICSNC 2012 technical program committee as well as the numerous reviewers. The creation of such a broad and high quality conference program would not have been possible without their involvement. We also kindly thank all the authors that dedicated much of their time and efforts to contribute to the ICSNC 2012. We truly believe that thanks to all these efforts, the final conference program consists of top quality contributions.

This event could also not have been a reality without the support of many individuals, organizations and sponsors. We also gratefully thank the members of the ICSNC 2012 organizing committee for their help in handling the logistics and for their work that is making this professional meeting a success. We gratefully appreciate to the technical program committee co-chairs that contributed to identify the appropriate groups to submit contributions.

We hope the ICSNC 2012 was a successful international forum for the exchange of ideas and results between academia and industry and to promote further progress in networking and systems communications research.

We hope Lisbon provided a pleasant environment during the conference and everyone saved some time for exploring this beautiful city.

ICSNC 2012 Chairs

ICSNC Advisory Chairs
Eugen Borcoci, University Politehnica of Bucarest, Romania
Sathiamoorthy Manoharan, University of Auckland, New Zealand
Reijo Savola, VTT, Finland
Leon Reznik, Rochester Institute of Technology, USA
Masashi Sugano, Osaka Prefecture University, Japan
Zoubir Mammeri, IRIT, France

ICSNC 2012 Research Institute Liaison Chairs
Song Lin, Yahoo! Labs / Yahoo Inc. - Sunnyvale, USA
Habtamu Abie, Norwegian Computing Center - Oslo, Norway

ICSNC 2012 Industry/Research Chairs
Rolf Oppliger, eSECURITY Technologies - Guemligen, Switzerland
Jeffrey Abell, General Motors Corporation, USA
Christopher Nguyen, Intel Corp., USA
Javier Ibanez-Guzman, RENAULT S.A.S. / Technocentre RENAULT - Guyancourt, France

ICSNC 2012 Special Area Chairs

Mobility / vehicular
Maode Ma, Nanyang Technology University, Singapore

Pervasive education
Maiga Chang, Athabasca University, Canada

ICSNC 2012

Committee

ICSNC Advisory Chairs

Eugen Borcoci, University Politehnica of Bucarest, Romania
Sathiamoorthy Manoharan, University of Auckland, New Zealand
Reijo Savola, VTT, Finland
Leon Reznik, Rochester Institute of Technology, USA
Masashi Sugano, Osaka Prefecture University, Japan
Zoubir Mammeri, IRIT, France

ICSNC 2012 Research Institute Liaison Chairs

Song Lin, Yahoo! Labs / Yahoo Inc. - Sunnyvale, USA
Habtamu Abie, Norwegian Computing Center - Oslo, Norway

ICSNC 2012 Industry/Research Chairs

Rolf Oppliger, eSECURITY Technologies - Guemligen, Switzerland
Jeffrey Abell, General Motors Corporation, USA
Christopher Nguyen, Intel Corp., USA
Javier Ibanez-Guzman, RENAULT S.A.S. / Technocentre RENAULT - Guyancourt, France

ICSNC 2012 Special Area Chairs

Mobility / vehicular
Maode Ma, Nanyang Technology University, Singapore

Pervasive education
Maiga Chang, Athabasca University, Canada

ICSNC 2012 Technical Program Committee

Habtamu Abie, Norwegian Computing Center - Oslo, Norway
João Afonso, FCCN - National Foundation for Scientific Computing, Lisbon, Portugal
Jose Maria Alcaraz Calero, Hewlett-Packard Research Laboratories - Bristol, UK
Pedro Alexandre S. Gonçalves, Escola Superior de Tecnologia e Gestão de Águeda, Lisbon
Abdul Alim, Lancaster University, UK
Sultan Aljahdali, Taif University, Saudi Arabia
Abdullahi Arabo, Oxford Internet Institute / University of Oxford, UK
Shin'ichi Arakawa, Osaka University, Japan
Ali Bakhtiar, Technological University of America - Coconut Creek, USA

Sokratis K. Katsikas, University of Piraeus, Greece
Pierre Kleberger, Chalmers University of Technology - Gothenburg, Sweden
Romain Laborde, University of Toulouse, France
Wolfgang Leister, Norsk Regnesentral (Norwegian Computing Center), Norway
Tayeb Lemlouma, IRISA / IUT of Lannion (University of Rennes 1), France
Hui Li, Shenzhen Graduate School/Peking University, China
Jian Li, IBM Research in Austin, USA
Kuan-Ching Li, Providence University, Taiwan
Yaohang Li, Old Dominion University, USA
Wei-Ming Lin, University of Texas at San Antonio, USA
Thomas Little, Boston University, USA
Edmo Lopes Filho, Algar Telecom, Brazil
Christian Maciocco, Intel, USA
Kia Makki, Technological University of America - Coconut Creek, USA
Amin Malekmohammadi, University of Nottingham, Malaysia
Zoubir Mammeri, IRIT, France
Herwig Mannaert, University of Antwerp, Belgium
Sathiamoorthy Manoharan, University of Auckland, New Zealand
Gregorio Martinez, University of Murcia, Spain
Yakim Mihov, Technical University of Sofia, Bulgaria
Karol Molnár, Honeywell International, s.r.o. - Brno, Czech Republic
Mohammad Mostafizur Rahman Mozumdar, California State University - Long Beach, USA
Peter Mueller, IBM Zurich Research Laboratory, Switzerland
David Navarro, Lyon Institute Of Nanotechnology, France
Ronit Nossenson, Jerusalem College of Technology, Israel
Rolf Oppliger, eSECURITY Technologies - Muri b. Bern, Switzerland
Péter Orosz, University of Debrecen, Hungary
Gerard Parr, University of Ulster-Coleraine, Northern Ireland, UK
Dennis Pfisterer, Universität zu Lübeck, Germany
Victor Ramos, UAM-Iztapalapa, Mexico
Leon Reznik, Rochester Institute of Technology, USA
M. Tahir Riaz, Aalborg University, Denmark
Joel Rodrigues, University of Beira Interior, Portugal
Enrique Rodriguez-Colina, Autonomous Metropolitan University – Iztapalapa, Mexico
Javier Rubio-Loyola, CINVESTAV, Mexico
Jorge Sá Silva, University of Coimbra, Portugal
Demetrios G Sampson, University of Piraeus & CERTH, Greece
Carol Savill-Smith, GSM Associates, UK
Reijo Savola, VTT, Finland
Marialisa Scatà, University of Catania, Italy
Axel Sikora, University of Applied Sciences Offenburg, Germany
Adão Silva, University of Aveiro / Institute of Telecommunications, Portugal

Copyright Information

For your reference, this is the text governing the copyright release for material published by IARIA.

The copyright release is a transfer of publication rights, which allows IARIA and its partners to drive the dissemination of the published material. This allows IARIA to give articles increased visibility via distribution, inclusion in libraries, and arrangements for submission to indexes.

I, the undersigned, declare that the article is original, and that I represent the authors of this article in the copyright release matters. If this work has been done as work-for-hire, I have obtained all necessary clearances to execute a copyright release. I hereby irrevocably transfer exclusive copyright for this material to IARIA. I give IARIA permission or reproduce the work in any media format such as, but not limited to, print, digital, or electronic. I give IARIA permission to distribute the materials without restriction to any institutions or individuals. I give IARIA permission to submit the work for inclusion in article repositories as IARIA sees fit.

I, the undersigned, declare that to the best of my knowledge, the article is does not contain libelous or otherwise unlawful contents or invading the right of privacy or infringing on a proprietary right.

Following the copyright release, any circulated version of the article must bear the copyright notice and any header and footer information that IARIA applies to the published article.

IARIA grants royalty-free permission to the authors to disseminate the work, under the above provisions, for any academic, commercial, or industrial use. IARIA grants royalty-free permission to any individuals or institutions to make the article available electronically, online, or in print.

IARIA acknowledges that rights to any algorithm, process, procedure, apparatus, or articles of manufacture remain with the authors and their employers.

I, the undersigned, understand that IARIA will not be liable, in contract, tort (including, without limitation, negligence), pre-contract or other representations (other than fraudulent misrepresentations) or otherwise in connection with the publication of my work.

Exception to the above is made for work-for-hire performed while employed by the government. In that case, copyright to the material remains with the said government. The rightful owners (authors and government entity) grant unlimited and unrestricted permission to IARIA, IARIA's contractors, and IARIA's partners to further distribute the work.

Table of Contents

Rifidi Toolkit: Virtuality for Testing RFID Systems

Andreas Huebner*, Christian Facchi* and Helge Janicke†
*Institute of Applied Research, University of Applied Sciences Ingolstadt, Germany
{andreas.huebner, christian.facchi}@haw-ingolstadt.de
†Software Technology Research Laboratory, De Montfort University, Leicester, United Kingdom
heljanic@dmu.ac.uk

***Abstract*—The Rifidi Toolkit is an open source framework for virtual Radio Frequency Identification (RFID) environments. It allows to emulate RFID devices and can be used as a basis for testing RFID applications. The concept behind the Rifidi Toolkit is already widely adopted in industry and has been accepted in science. This paper gives an introduction on the the toolkit's architecture and design. It further points out how to use the toolkit for testing RFID applications and proposes new features and functionality needed for robust RFID application testing with the Rifidi Toolkit.**

Keywords-RFID; test-data generation; software testing; virtualisation; Rifidi

I. Introduction

RFID [1] is gaining momentum in industry as an increasing number of RFID applications are deployed. The trend towards automatic identification of objects also increases the demand for qualitative and fail proof RFID applications. Therefore research on testing RFID systems speeds up and methodical approaches on testing RFID systems are needed. Even though most publications on testing RFID focus on performance evaluation, a commonly encountered problem with all approaches on testing RFID, is that it is very expensive to fund the physical RFID test environment. To address this problem the Rifidi Toolkit [2] was developed. The toolkit allows to virtualise the RFID environment, therefore, drastically reduce the test costs and in consequence also reducing the overall project costs.

This paper gives an introduction into the open source framework Rifidi and shows the design ideas behind the software. It points out what features are required to use the toolkit for testing RFID applications. Furthermore, it exposes additional improvements to the Rifidi Toolkit, so it can be applied as a basis for functional testing of RFID applications.

The remainder of the paper is structured as follows: In Section II, an overview of the tools included in the Rifidi Toolkit is given. The *Emulator Engine*, the central part of the toolkit, is explained in detail in Section III. Then, the architecture of the different modules is explained in Section IV. An introduction to requirements for testing RFID is given in Section V. Section VI presents the related work and shows the acceptance of the Rifidi Toolkit and the principles behind it. Drawbacks and proposed enhancements can be found inSection VII. Finally, a conclusion and a future perspective are given in Section VIII.

II. Rifidi Toolkit Overview

The Rifidi Toolkit enables the virtualisation of RFID readers of various vendors for flexible and improved testing of RFID applications. Utilizing virtual RFID readers in this context means less physical readers need to be available for testing. Therefore, it lowers the barrier to enter the RFID world and allows to save resources and time. The Rifidi Toolkit is available since 2006 as open source software on SourceForge.net [3] and already established on the market as a valuable resource for many users, which can be seen on the number of downloads (over 50,000 since 2006 [4]).

The Rifidi Toolkit consists of three software tools; namely the *Emulator*, the *Designer* and the *TagStreamer* [5]. All these are based on the *Emulator Engine*, the central part of the Rifidi tool-suite which is capable of emulating virtual RFID devices.

Emulator - The Rifidi Emulator is a graphical interface for controlling and interacting with virtual readers. It allows the emulation of readers and tags as well as read and write events. Additionally, it provides access to the virtual readers like their physical counterparts.

Designer - The Rifidi Designer is a tool to build custom 3D production environments, that can be used for visually simulating the RFID data flow. It is also based on the *Emulator Engine* and allows the emulation of RFID readers and the interaction with them. It is not actively maintained anymore but can still be accessed on the SourceForge.net website.

Tag Streamer - The Rifidi Tag Streamer is a performance testing tool that allows to generate large numbers of virtual readers and tags to evaluate the RFID system.

III. The Rifidi Emulator Engine

The *Emulator Engine* is the core part of the Rifidi Toolkit. It is responsible for managing and controlling the emulation of the RFID devices. One Instance of the *Emulator Engine* can control multiple virtual readers of various vendors at the same time. All parts of the Rifidi Toolkit are implemented in Java and use different technologies around the Eclipse Framework, e.g Equinox, JFace and SWT.

The basic tasks of the *Emulator Engine* are:

- Handle communication between RFID reader and client
- Execute commands issued to the virtual reader
- Management of the antennas and the related field of sight
- Control the reader specific components, like signals on the *general purpose input/output* ports (GPIO ports)

 ISBN: 978-1-61208-231-8

Because of a Service Oriented Architecture (SOA) [6] approach, the functionality of the *Emulator Engine* is distributed in two core services. These services can be obtained through the *ServiceRegistry* and used to manage virtual readers, virtual tags and keep track of the tags in the Rifidi Environment.

ReaderManager - This service is responsible to manage the devices and offers of the following actions:

- Create a virtual reader
- Delete a virtual reader
- Start a virtual reader (power on)
- Stop a virtual reader (power off)
- Add a virtual tag to a reader's field of sight
- Remove a virtual tag from a reader's field of sight
- Get a list of virtual tags currently in the readers field of sight

IRifidiTagService - This service is used to create and handle virtual tags. It consists of the following functionality:

- Create a virtual tag
- Delete a virtual tag
- Track virtual tag data changes

All existing Rifidi tools are based on the *Emulator Engine* and allow an intuitive, graphical access to the presented functionality. However, the Rifidi Toolkit can also be used as a basis for other tools, which rely on the emulation of virtual RFID devices, e.g., test data generators. But, to use the capabilities of the tool-suite for improved testing of RFID applications, a better insight on the framework is necessary.

IV. Emulator Engine Architecture

This section gives more insight on the architecture of the Rifidi tool-suite and describes how to use this architectural model as a basis for virtual readers. It concludes with an overview of the command flow through the *Emulator Engine*.

A concrete implementation of a virtual reader is called *reader module*. To seamlessly integrate into the framework each *reader module* implements interfaces of the components, presented below.

The architecture of the *Emulator Engine* is based on the structure of a physical RFID reading device. The idea was to develop the virtual readers similar to their physical counterparts and therefore to use the same logical components. Figure 1 gives an overview of the different components of the *Emulator Engine*. Each box represents a logical counterpart of a physical reader and can be seen as a generally valid abstract component of all virtual readers.

A. Emulator Engine Components

The components of the *Emulator Engine* are Communication, Command Processor, Radio, General Purpose Input/Output and Shared Resources. The different tasks and functionalities of the virtual reader's components are explained in the following:

Communication - Even though most modern RFID devices use an Internet Protocol (IP) connection for communication,

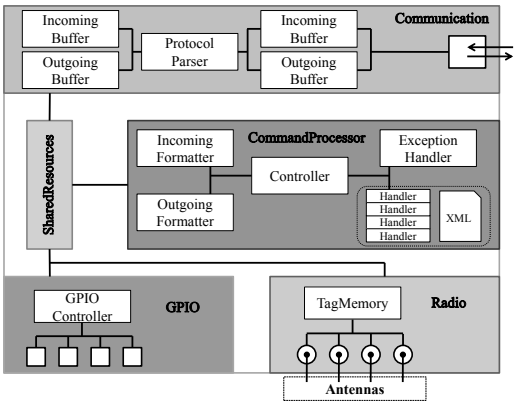


Figure 1. Emulator Engine Architecture Overview [5]

there are still some vendors using other interfaces like serial link, e.g., RS232, or other proprietary ones. To map these diverse ways of communication to the framework a generic communication part for each virtual reader needs to be considered. In the Rifidi environment this is realized through the communication component. It enables receiving and sending of messages as well as forwarding the encoded messages to or respectively from the command processor. The communication is divided into two parts:

Protocol Parser: The protocol parser converts the messages received in binary format to a message the command handler can deal with. This can be either a reader specific message format or an plain Java object. The *Protocol Parser* is also used this way when it converts a message from the command handler to a binary message, which can be sent through the reader specific communication. With respect to IP-based communication, especially regarding fragmented packets, the parser is also responsible to determine if a messages was received completely.

Buffer: The buffer is used to store messages and enable asynchronous communication from the communication channels. There is one buffer for incoming and outgoing messages.

Command Processor - The interaction with common RFID readers is based on command/response protocols. Subsequently the issued commands need to be parsed, executed, and finally, responded. In the Rifidi environment, the command processor can be seen as the central processing unit and is used for this purpose. For each command it invokes the appropriate methods of the virtual reader. A list of commands and the corresponding actions, implementing the functionality of the command, are defined in a XML file called `reader.xml`. The Rifidi framework utilizes *Java Reflections* [7] to execute the classes and methods specified in this XML file. The command processing layer is consisting of three parts:

Formatter: As for the buffers, there are formatters for each direction of communication. The incoming formatter is used to strip and decompose the commands. Usually, the first parts of a command determine the command type, all

 ISBN: 978-1-61208-231-8

additional information are arguments and parameters. The outgoing formatter assembles outgoing messages for further processing in the communication layer.

Controller: The controller, also called command handler, is the central processing unit for commands. Each command issued to the virtual reader is executed here. The *HandlerMethods* are invoked through reflection.

Exception Handler: The exception handler is a special *HandlerMethod*, which takes care of unknown, undefined or misspelled commands. Usually, error descriptions are send back to provide feedback.

Radio - The radio component represents the air interaction capabilities of the virtual RFID device and allows to interact with virtual tags. In the Rifidi Emulator, for example, a user can control when a tag is added to an antenna or when a tag is removed. Additionally, to the users interaction the reader can also, depending on the reader capabilities, write or read the tag. Furthermore, it is vendor specific how ”tag events” are stored and handled in a reader, therefore each virtual reader has its own radio component and memory structure. As an example, the *Alien 9800* (Alien Technology Corporation) RFID reader allows either to list all read events since the last poll or to list just the currently available tags in the field of sight.

Tag Buffer: The tag buffer implements the memory structure and the over-the-air interaction capabilities of the virtual reader. The Tag Buffer is associated to the virtual antennas of a reader. The antennas represent the interfaces for the *Emulator Engine* to simulate RFID tag operation events. It has to be distinguished between read and write operations. Reading tags means a tag's information was read by the reader and writing tags means the tag was modified during time the tag was available in the field of sight. An Event is either a tag appears on the antenna or disappears. In more detail, this means a list of virtual tags is either added to the antenna or removed from the antenna.

General Purpose Input/Output - Some RFID devices allow additional sensors to be connected to it. This is widely known as *General Purpose Input/Output* (GPIO) and realised as small electrical connectors on the RFID reader. The presence of GPIO ports is also reader specific and the virtual functionality is provided by this part. Currently, only the Low Level Reader Protocol (LLRP) Reader and the Alien 9800 Reader leverage this functionality in the Rifidi Framework, yet.

Shared Resources - The shared resources are used as a housekeeping component for each virtual reader. It is a central instance holding together the different components and allowing to transfer data objects from the above described layers in this section.

B. Overview of the Command Flow

Concluding with the different components of an virtual reader, Figure 2 gives an overview of the command flow through the different parts of the *Emulator Engine*. It shows a schematic view of the data exchange and interactions of the different components. The dotted lines around the components indicate implementation specific parts, which can be different in each virtual *reader module*. All incoming commands are

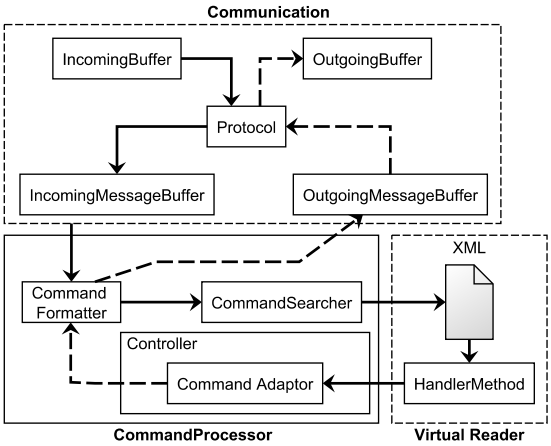


Figure 2. Rifidi Command Flow Overview [5]

received by the *IncomingBuffer*, encoded in a binary format. Once all bytes of the message are read, it is forwarded to the *Protocol*. The *Protocol* decodes the binary messages to a processable format and hands it further to the *IncomingMessageBuffer*. The *IncomingMessageBuffer* stores the Message until the *CommandProcessor* is available for processing. The *CommandProcessor*, consisting of the *CommandFormatter*, the *CommandSearcher* and *CommandAdapter*, is parsing the message and looking up the corresponding *HandlerMethod*. Finally the located method is executed and the intended actions are performed. If there is a response or a result of the previously executed command the data is going through all components again in reverse order. Following the dotted arrows, the reply first goes through the *CommandFormatter* again. Afterwards, it is given to the *OutgoingMessageBuffer*, then encoded by the Protocol, and finally, sent to the *OutgoingBuffer*.

V. Requirements for testing RFID

In this section, an overview of a generic RFID system is given. Based on the description of the sketched system, a transformation into a virtual system is performed, while both systems are used to demonstrate the testing capabilities. Finally, constraints as well as requirements to be fulfilled for testing with the virtual system are listed.

A. Structure of a simplified RFID system

A simple RFID system is composed of one or more RFID readers, a RFID middleware and an application. The RFID tags are usually attached to objects the RFID system is interested in. Once an object with an attached RFID tag gets close to a reader's antenna the tag will be read. This is often referred to as a tag read event. As long as the tag stays in the field it can also be written, which is then referred as write event.

 ISBN: 978-1-61208-231-8

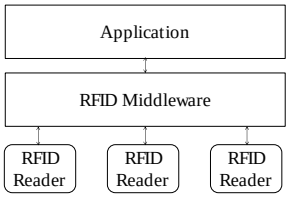


Figure 3. RFID System

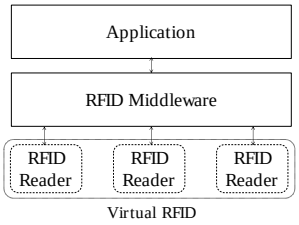


Figure 4. Virtual RFID System

Figure 3 shows a schematic RFID system and the interaction between the components. RFID Tags are read on the antennas of the reader and reported to the middleware. This middleware filters redundant data, applies logical evaluations and generates business events for the RFID application.

To test a system like this, certain RFID events, usually read events, need to be generated. These events will then be processed by the middleware and finally handed to the RFID application. Depending on the business logic of the application a specific result is produced.

In today's practical testing approaches the generation of tag read events is produced by someone walking through the readers field of sight. The resulting effects in the application are then evaluated.

B. Virtuality for testing RFID

To improve the manual test process the real world devices can be substituted by virtualised RFID, with virtual readers from the Rifidi Toolkit, with an otherwise unchanged tool chain. From the perspective of the RFID middleware and application the simulated system cannot be distinguished from a real system. This "virtuality"-system can even be a system composed of randomly mixed real and virtual devices. Figure 4 shows the changed RFID system. In this case, all RFID devices have been substituted by virtual readers. A tester can now place virtual tags on the virtual readers, and therefore, generate the same input as with the previously described real environment.

C. Testing with Rifidi

To enhance testing with this "virtuality"-system and enable automatic testing, the newly created virtual environment needs to be instrumented. For the instrumentation of the virtual environment a new test controller can be used. In the Rifidi Toolkit this functionality could be provided by a new tool using the *Emulator Engine* to map the movements of tags in the real world. However, to test RFID applications a missing part is still the automatic evaluation of the RFID middleware respectively the application. This is a challenging task because of the diverse variety of RFID applications. Compared to middleware systems, where the *Application Level Event* (ALE) [8] standard can be used to communicate and evaluate the test results, for each application an evaluation adapter needs to be implemented. Additionally, to the missing interface, to evaluate the test results in applications, even more complexity is introduced by the attributes of RFID data. According to [9] RFID data consists of a data stream with the following attributes:

- Redundant Data
- Grouped Data
- Moving Route
- Noisy Data

These parameters need to be considered during the generation of test data. Rifidi supports most of the requirements in its virtualisation of RFID readers, however, it is notably lacking support to model events that occur due to physical effects such as interference and timing delays. As part of our ongoing research, we are investigating realistic interference models and also work on real-time aspects of RFID testing.

VI. Related Work

Since 2006, when the framework was published on SourceForge.net, it has been downloaded over 50,000 times [4] and used by developers, teachers and researchers. The Rifidi Toolkit has been referred in many publications, which shows the significance of the presented tool. Furthermore, in this paper we presented the architectural consideration and the requirements that underpin the current implementation of Rifidi to enable an even more widespread adoption of the framework in particular with the view of using Rifidi in the Quality Assurance of RFID applications.

However, there are similar developments capable to emulate virtual RFID readers. This section covers some of the approaches and points out what the differences of the implementations are. Additionally, it shows where the Rifidi Toolkit was used in science, research, education and industry.

A. Comparable RFID Emulators

Currently there are two implementations of virtual RFID emulators mentioned in scientific publications, but unfortunately neither the *Virtual Test Toolkit* from the Pusan National University nor the *RFID Performance Test Tool* from the Feng Chia University was available for download and comparison. Hence, the further statements are only based on information which could be obtained from publications and not from concrete experiments.

Pussan National University (PNU LIT) - [10], [11], [12], [13] describe a virtual reader emulator to evaluate a RFID Middleware mainly with the focus on performance issues. The Toolkit is divided into three parts; the *Virtual Application Emulator*, the *Virtual Device Emulator* and the *Toolkit Operator*. Where the *Virtual Device Emulator* is comparable to the Rifidi Toolkit. It is capable to emulate one or more virtual RFID readers and virtual RFID tags. The virtual readers can interact with the virtual tags, which are following the EPC Global Data Tag Standard. The *Toolkit Operator* controls the virtual environment and is the central part of the Virtual Test Toolkit. The *Virtual Application Emulator* is connected to the RFID Middleware and acts as a RFID Application. The purpose of the *Virtual Application Emulator*

is to collect information regarding the performance of the middleware under test for performance evaluation purposes. The toolkit was firstly published in 2009 [10] and follows the similar objectives than the Rifidi Toolkit and the RFID Performance Test Tool. It differs to the Rifidi Toolkit mainly in the emulation's level of detail. For example, a fine grained access to the virtual readers including configuring the output format of tag events seems not to be possible. Nevertheless, it can be used as a basis for testing, but it is not as flexible as the Rifidi Toolkit.

Feng Chia University (FCU RFIDLab) - Jongyoung and Naesoo [14] introduce the design and implementation of a Performance Test Tool for RFID middleware, consisting of a test data generator and a result data estimation part. The test data generator supports different tag data standards and various reader protocols, e.g. from EPC Global, Alien Technology and Motorola (former Matrics). The result data estimation part implements the ALE specification and connects to the RFID middleware, which is the *Software Under Test* (SUT), as a virtual application. The reader emulator, which is part of the test generation tool, is controlled via a graphical user interface and allows to specify how many tags will be generated. Additionally to the amount of tag events the simulation should generate, it allows to specify a pattern for the encoding of the generated tag data and a timing interval for the events. After the previously specified test data was generated, it is accessible for the RFID Middleware through the "result data transmission"-part. Summarized the introduced tool is similar to the concept of the Rifidi TagStreamer. It is a performance test tool to test RFID Middleware and allows the emulation of vendor specific reader protocols. But, different to the TagStreamer, it does not allow a fine grained access or interaction with the virtual readers. Nevertheless, the advantage of the Performance Test Tool is the result estimation part, which is used as the upper tester of the test suite.

Hardware Emulators - Beside the software emulators, there is also a variety of physical emulators available. The hardware emulators are mainly used to simulate RFID readers, in order to test new air protocols, modifications to existing protocols and new command sets. But, some of the devices can even simulate RFID tags. For example, CISC Semiconductors offers the *RFID Tag Emulator* [15], a mobile device capable of emulating multiple RFID tags. This tag simulator can be used to analyse and test RFID Reader performance with certain tag populations. But, similar to real RFID readers these simulators come with the same limitations, regarding the high investment costs, compared to virtual readers. This downside is especially obvious for performance testing, where a huge number of devices is needed.

B. Publications about Rifidi

The concepts of the Rifidi Toolkit have been discussed in many publications. A not exhaustive list of publications around the Rifidi Toolkit is given in this section:

Palazzi and Ceriali [16] provided a critical investigation of the capabilities of the Rifidi Toolkit regarding RFID system testing. For this investigation they use the toolkit in a case study to demonstrate the current potentials. Siror et al. [17] use Rifidi as a basis to evaluate the usability of an an automatic evaluation of a customs verification process. In both cases the Rifidi framework was successfully used to simulate the RFID environment and therefore supported the fast and easy demonstration of the case studies. Mueller et al. [18] compare different test data generators and conclude, that the Rifidi Toolkit is an specialized data generator which can generate RFID events by emulating RFID readers.

C. Applications in Science, Education and Industry

The Rifidi Toolkit is not only used in research, it is also used in many different other areas. Rifidi provides enormous benefits especially for industry and education. The reason to use the virtual RFID environment here is mainly because of the reduced costs and the availability of readers. In summary, researchers, scientists and teachers can work with RFID readers without having the budget for the hardware and neither to argue with their colleagues when the device is available. As far as it is known to the knowledge of the authors the University of Applied Sciences Ingolstadt and University of Applied Sciences Regensburg are using the toolkit beside others [19] for educational purposes.

But, the previous mentioned benefits are also valid for industrial users. The Rifidi Toolkit is used for a wide variety of industrial applications and helps companies to realise RFID projects faster with less costs. Some of the users known to the authors are BMW, HP and IBM.

VII. Enhancements for Rifidi

The Rifidi Software can be used as a basis for testing RFID applications and its infrastructure. To truly match the requirements for testing, some improvements to the framework need to be made. Four categories can be distinguished:

Reader Support - To keep the virtual RFID framework up-to-date it is necessary to map the changes in the development of physical readers to the Rifidi framework. Even when the *Emulator Engine* already supports a great variety of readers and appropriate reader protocols the framework could be enhanced by adding more readers to it. Integrating new virtual readers is a lot of effort, especially because vendors usually do not provide the necessary information. Therefore, typically, a reader has to be reverse engineered for implementation purposes. Not only the time it takes, but also the cost of the hardware needs to be taken into account. As a result, better guidelines and methodologies to enhance the software development of the Rifidi suite have to be found.

Tag Creation - Another drawback in the Rifidi Environment is the generation of virtual tags. Currently, the creation of tags is based on random numbers which are grouped by the means of the encoding, like *Serialized Global Trade Identification Number* (SGTIN). According to Zhang et al. [9], one can distinguish between *Semantic Invalid Data* (SID) and *Semantic Valid Data* (SVD). Whether to use SID or SVD depends on the

 ISBN: 978-1-61208-231-8

test objective. For example, SID is used when the performance of an system needs to be evaluated. In this case the meaning of the data is irrelevant for the test objective. To test functional aspects of RFID middleware or applications the identifiers used in the simulation need to have a semantic meaning determined by SVD. The semantic meaning expresses the relationship between the tag's identifier and the actual object the tag is attached to. Therefore, the tag's identifiers need to be associated with the actual serial numbers an application's database stores. This can either be achieved by establishing a connection to the database, an interface to the system, respectively an adapter, or with a manually instrumented set of tag patterns during the creation of tags.

Robustness and Stability - A necessary attribute of software used for testing is that itself does not introduce errors and failures. Therefore, using the Rifidi Framework as a basis for testing RFID systems also leads to the question: Is the software stable and reliable enough to truly be the basis for testing? Concepts and studies concerning this issue need be made and show that Rifidi is fulfilling these requirements.

Scripting and Automatic Execution - Currently, the Rifidi Framework exposes its functionality through the three tools with GUI's. To enable more complex testing, the framework need to be instrumented by a test manager. This could be achieved by introducing scripting support for the automatic execution of tag movement patterns. The scripting language could be a domain specific language to easily match the requirements for testing RFID applications and their functionality.

VIII. Conclusion and Future Work

The Rifidi Toolkit is virtual framework for the simulation of RFID devices. The architecture is based on the real layout of physical RFID readers and allows a fine grained access to the virtual RFID readers like their physical counterparts. It serves as a framework for the implementation of many different readers with its flexible and general layout. Some of the principles behind the Rifidi architecture seem to be already adopted in different areas of science and industrial use. Furthermore, it is a basis for further research and allows testing of RFID applications. The Rifidi Toolkit can be extended to improve testing capabilities and support modern testing techniques.

Physical Effects on the Air Interface - A drawback, which can be a task for future work, is that none of the presented software tools truly cover the physical constraints of the air interface. In reality, each RFID reader is susceptible for missing tag reads. To be able to truly test RFID environments the physical effects in the *radio frequency* (RF) field have to be taken into account. This means the RF field and its effects also need to be simulated in the emulation of the RFID readers. An approach could be to introduce heuristics and statistical based reasoning functions, which need to represent the physical constraints more closely. But, furthermore, also the impact of missed tag readings on the RFID application with regard to testing has to be researched.

IX. Acknowledgements

The authors would like to thank the Software Technology Research Laboratory (STRL) and the Faculty of Technology of the De Montfort University, especially Peter Norris and Stephen Ison for providing the appropriate environment for research. This research has been funded by project grants from the German Federal Ministry of Education and Research (BMBF). Project: ITERA, FKZ 01QE1105B.

References

[1] K. Finkenzeller, *RFID-Handbook, 3rd edition*. Wiley, 2010.

[2] Pramari LLC, "Rifidi Project," online: http://www.rifidi.org, 2006, [accessed: December 14, 2011].

[3] ——, "Rifidi - from rfidea to business reality," online: http://sourceforge.net/projects/rifidi/, 2011, [accessed: March 28, 2011].

[4] ——, "Rifidi Statistics," online: http://sourceforge.net/projects/rifidi/files/stats/timeline?dates=2005-01-05+to+2012-07-02, 2012, [accessed: June 01, 2012].

[5] ——, "Rifidi Emulator Documentation: Developers Guide," online: http://wiki.rifidi.org/index.php/Engine_Overview, 2008, [accessed: December 14, 2011].

[6] R. Perrey and M. Lycett, "Service-oriented architecture," in *Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on*, jan. 2003, pp. 116 – 119.

[7] G. McCluskey, "Using java reflection," online: http://java.sun.com/developer/technicalArticles/ALT/Reflection/, 1998, [accessed: June 12, 2012].

[8] EPCglobal inc., "The application level events (ale) specification, version 1.1.1," online: http://www.gs1.org/gsmp/kc/epcglobal/ale/ale_1_1_1-standard-core-20090313.pdf, 2009, [accessed: June 05, 2012].

[9] H. Zhang, W. Ryu, B. Hong, and C. Park, "A test data generation tool for testing rfid middleware," in *Computers and Industrial Engineering (CIE), 2010 40th International Conference on*, july 2010, pp. 1 –6.

[10] C. Park, W. Ryu, and B. Hong, "RFID Middleware Evaluation Toolkit Based on a Virtual Reader Emulator," in *Emerging Databases, The 1th International Conference on Emerging Databases 2009*, 2009, pp. 154–157.

[11] G. Lee, H. Zhang, C. Park, W. Ryu, and B. Hong, "Design and Implementation of Virtual Test Toolkit for Testing RFID Middleware," in *Intelligent Manufacturing and Logistics Systems, The 6th International Conference on IML 2010*, 2010, pp. 1–6.

[12] H. Zhang, W. Ryu, B. Hong, and C. Park, "A test data generation tool for testing rfid middleware," in *Computers and Industrial Engineering (CIE), 2010 40th International Conference on*, 2010, pp. 1–6.

[13] J. Park, W. Ryu, B. Hong, and B. Kim, "Design of toolkit of multiple virtual readers for scalability verification of RFID middleware," in *The Second International Conference on Emerging Databases (EDB 2010)*, 2010, pp. 56–59.

[14] L. Jongyoung and K. Naesoo, "Performance test tool for rfid middleware: Parameters, design, implementation, and features," in *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference*, vol. 1, feb. 2006, pp. 149 –152.

[15] C. Semiconductors, "Rfid tag emulator," online: https://www.cisc.at/?id=25, 2012, [accessed: June 05, 2012].

[16] M. D. M. C. E. Palazzi, A. Ceriali, "RFID emulation in Rifidi Environment," in *International Symposium on Ubiquitous Computing (UCS'09)*, 2009.

[17] J. Siror, S. Huanye, and W. Dong, "Automating customs verification process using rfid technology," in *Digital Content, Multimedia Technology and its Applications (IDC), 2010 6th International Conference on*, aug. 2010, pp. 404 –409.

[18] J. Müller, M. Schapranow, C. Pöpke, M. Urbat, A. Zeier, and H. Plattner, "Best practices for rigorous evaluation of rfid software components," in *RFID Systech 2010, RFID Systech 2010 - European Workshop on Smart Objects: Systems, Technologies and Applications*, 2010.

[19] Transcends LLC (former Pramari LLC), "Academic partners," online: http://www.transcends.co/partners/academic, 2011, [accessed: June 03, 2012].

 ISBN: 978-1-61208-231-8

Address Resolution in Mobile Ad Hoc Networks using Adaptive Routing

Thomas Finke, Juergen Schroeder
Department of Electronics and Information Technology
Heilbronn University, Germany
{thomas.finke,juergen.schroeder}@hs-heilbronn.de

Sebastian Schellenberg, Markus Hager, Jochen Seitz
Communication Networks Group
Ilmenau University of Technology, Germany
{sebastian.schellenberg,markus.hager,jochen.seitz}@tu-ilmenau.de

***Abstract*—In disaster scenarios, communication systems usually consist of heterogeneous nodes and damaged infrastructure. Communication is important for rescue teams and victims as well but a serious problem because normal network systems like wired or mobile radio Internet could be unreliable or simply not available. To deal with these problems, much effort has been spent to mobile ad hoc networks (MANETs) and their specialties. Those networks are usually unsteady and highly mobile. Therefore, classical network services like resolution of names to their regarding local IP addresses is a big challenge. In this paper, we present our new approach for consistent and efficient name resolution using adaptive routing techniques. With this approach, routing and name resolution can be combined to decrease the latency of the lookup and to reduce the caused traffic.**

***Index Terms*—MANET; name resolution; adaptive routing.**

I. Introduction

A lot of applications in networks, nowadays, use names to address communication partners because it is easier for human users to remember names instead of numbers. For example, if someone wants to access a website, the web browser gets a Uniform Resource Locator (URL) and has to resolve this name to an IP-address. The mapping between such names (e.g., hostnames) and numbers (network addresses) in the Internet is done via the well known Domain Name System (DNS) [1] with centralized DNS servers.

A big problem in mobile ad hoc networks (MANETs) is the possibly high mobility and also the unreliability of nodes. For example, nodes can fail or simply go out of range. DNS is designed for infrastructure networks with centralized servers and is therefore not suitable for highly dynamic MANETs. If the centralized DNS server would fail, the whole MANET would be unable to resolve names. Therefore, mechanisms to prevent single points of failure must be developed.

MANETs have limited bandwidth and energy resources. Therefore, the communication protocols should only sparingly use a node's resources. To achieve this, we piggyback name resolution messages in routing packets to avoid additional traffic.

As the network topology can change in a wide range in highly dynamic MANETs, because of changing node speed or power resources for example, it is not very efficient to use only one routing protocol for all network constellations. Hence, we use an adaptive routing framework in our system to switch between different routing protocols during runtime and to achieve best performance in multiple network constellations by selecting the optimal routing protocol to a given network scenario. In our system, we use one reactive and one proactive routing protocol, however it is possible to integrate more than two routing protocols in our adaptive routing framework.

Our name resolution in reactive routing scenarios is inspired by Engelstad et al. [2] (cf. II-B). In proactive routing scenarios, we use our new proactive name resolution approach as discussed later in Section III-B, which allows hostname to address resolution and route finding without any latency for the sending application if the system has already learned the topology.

A challenging problem in MANETs are the rapidly changing network addresses of nodes in scenarios with high mobility, due to nodes that continuously enter, leave, or change the network. The founders of the Internet did not consider that there could be so many Internet using devices with high mobility, e.g., smartphones or laptops. That is why the Internet Protocol (IP) address is a locator and an identifier at the same time. If a node changes its location, it gets a new IP address, even if the identification remains the same.

The idea to solve this problem is to introduce a logical addressing scheme on top of IP to split the locator and identifier functionality. This splitting is well known in literature (e.g., [3]). However, mapping an identifier to a locater requires a working name resolution mechanism optimized for MANETs.

This paper shows our decentralized, fully distributed approach for name resolution using adaptive routing techniques. In Section II, we discuss related work regarding adaptive routing and existing name resolution approaches followed by our motivation for a new approach. Section III shows details about our name resolution system and about the used message types. We also show how our approach is transparent to the application and how names can be resolved over external networks.

II. Related Work

A. Adaptive Routing

In MANETs, the choice of the right routing protocol is important. We can divide the routing mechanism into two basic groups, the proactive and the reactive protocols. Proactive

 ISBN: 978-1-61208-231-8

routing protocols calculate the routes before they are needed. Therefore, the nodes exchange their routing information continuously. This is performed periodically or with every change in the topology. The proactive approach provides lower delays if a node wants to establish a connection. The drawback is the higher traffic caused by this strategy. One example is the well known Optimized Link State Routing (OLSR) protocol [4]. In systems with high mobility, this approach is not advisable.

In reactive or on-demand routing protocols, nodes only ask for routes when they need them. Therefore, the nodes do not have full knowledge about the whole network. This approach decreases the cost of synchronization but increases the delay for establishing a connection. An example is the Ad-hoc On-demand Distance Vector routing protocol (AODV) [5]. This type of routing algorithm is used in scenarios with high mobility and rapidly changing topologies.

In disaster scenarios it is difficult to assess which routing protocol is the best. Due to changing topologies and scenarios, the preferred routing protocol could change over time. If the positions and the connections of the nodes are stable, a proactive approach is best. If the nodes begin to move frequently, the reactive routing is better [2]. To provide the best protocol with respect to the current situation, adaptive routing allows to switch between different protocols. In our system, we use adaptive routing techniques to optimize routing and thus the efficiency of name resolution messages, which are piggybacked on routing packets.

Related work in that field has been done by Nanda et al. [6]. In this work, the nodes can switch between different routing protocols whereas these protocols do not have to be modified. The drawback of this work is that all nodes in the MANET have to use the same routing protocol at the same time and that the routing table entries have to be copied each time the protocol is changed. Another work was done by Hoebeke et al. [7], where each node can choose the best routing protocol for its requirements. Also multiple routing protocols are possible at the same time and a node does not have to support all used protocols. However, the drawback is that the used routing protocols have to be modified before they can be used in this framework. A further alternative is the hybrid Zone Routing Protocol [8] (ZRP), which provides a reactive and a proactive routing zone for each node. The nodes are able to modify the radius of their zones and, therefore, the ZRP also changes between different routing protocols to a certain degree.

B. Name Resolution Mechanism

In wired communication systems or scenarios with a robust infrastructure, name resolution is usually done by the well known Domain Name System [1]. One task in our system is to map the host names of the nodes to their current local network address or addresses if they are multi homed. It is obvious to use DNS for that, too [9]. But, in MANETs, the use of a centralized entity is difficult, because single points of failure could crash the whole system. There are three main approaches to adapt the DNS approach to MANETs. The first is to use centralized, but modified DNS [10]; second option is using multicast based approaches [11]; the third way is using routing techniques [2].

The Zeroconf Working Group has proposed a multicast based protocol for name resolution and service discovery in networks without conventional DNS servers [11]. Multicast DNS (mDNS) uses a multicast group with a well known multicast address for name resolution. Every node that wants to know the network address, which corresponds to a given name sends a request to that multicast address and the corresponding node answers the request with its network address. The drawbacks of mDNS are that an extra protocol for name resolution is needed and that a lot of additional traffic is produced because of flooding name requests to multicast addresses.

One idea of getting away from DNS is the routing-based approach proposed by Engelstad et al. [2], where the idea is to see the name resolution as a similar problem of finding a route. Instead of finding the local network address for a hostname and then in a second step finding a route, the approach asks for both at the same time (cf. Figures 1 and 2).

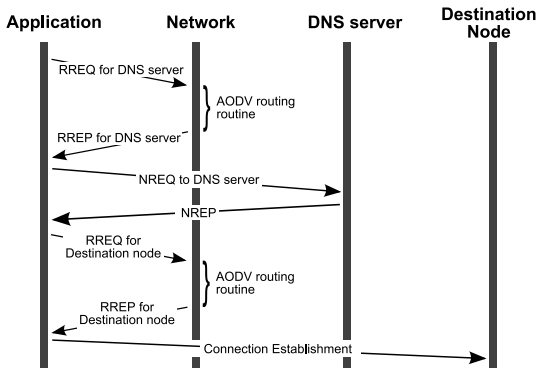


Fig. 1. Message sequence chart of connection establishment with reactive routing protocol

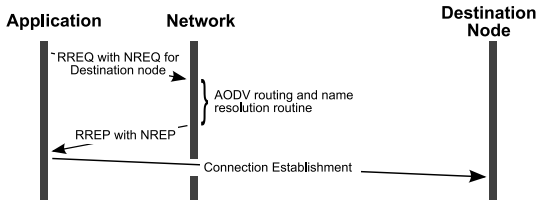


Fig. 2. Message sequence chart of connection establishment with reactive routing protocol and name resolution extension

Engelstad uses the reactive AODV routing protocol and sends the name resolution requests (NREQ) and replies (NREP) piggybacked with the route request (RREQ) and reply (RREP) messages [12]. Because of the combined name resolution and route finding approach, the packet overhead and the time between the need of an application to send data and the time where the first data packets can be transmitted is reduced. Nevertheless, this approach is limited to reactive routing approaches and can therefore not be used efficiently in

 ISBN: 978-1-61208-231-8

adaptive routing frameworks without a counterpart for proactive routing. In our system, we adapt Engelstadt's approach with some changes and introduce a proactive method. Details are shown in the next section.

III. Our Name Resolution over Adaptive Routing Approach

A. Adaptive Routing

As mentioned above, a specific routing protocol performs only well in one special network scenario. To cope with highly dynamic MANETs, our adaptive routing system switches between the two routing protocols AODV and OLSR. Therefore, a monitoring agent is used, which gathers information about the network state. This information is used by a decision maker, which selects the current routing protocol by operating selector switches, which control the routing packet flow. For coming to a decision, the module has access to the routing mode information telling what protocol should be used. Every node distributes its routing protocol decision inside an additional packet header throughout the network. Each implemented routing protocol uses its own independent routing table to store routes. The data packet forwarding module accesses the information inside the routing tables through a routing table wrapper, which looks inside all routing tables. The overall memory consumption of the routing tables is held low as a result of the dynamic memory allocation of the routing protocols. If a route's lifetime expires, the route is deleted and the memory is freed.

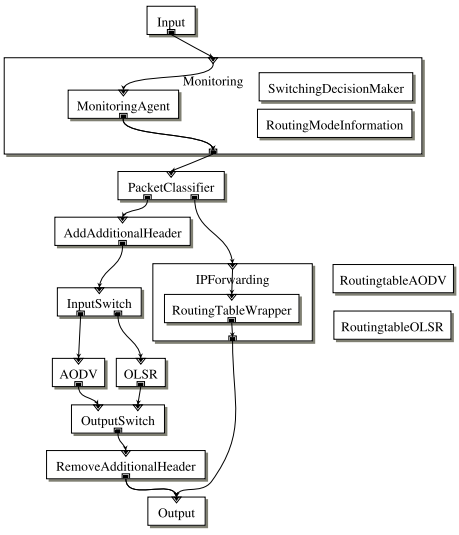


Fig. 3. Block Diagram of the Adaptive Routing Framework

We can switch to the reactive routing protocol when nodes are highly mobile and there are long communication sessions or we can switch to the proactive one when there are only some sporadic connections. Of course, we are not limited to implement only two routing protocols, our system is also able to support many different strategies as well. In this way, our routing performs well in a couple of network scenarios and outperforms prior routing approaches, which can only perform well in one special scenario.

B. Name Resolution via Proactive Routing

To avoid centralized DNS servers for resolving hostnames to network addresses, we use a decentralized routing-based approach, where each node is part of the name resolution system. For increasing the network performance during proactive operation, in terms of reducing the routing overhead and the latency for name resolution and route finding, we combine the name resolution mechanism with the routing protocols. Each node stores additional information about the mapping between hostnames and network addresses.

This subsection describes our proactive approach to resolve names to addresses. The names are usually human readable names to make it easier for users to identify nodes. If an application wants to resolve a name, it has to know this name. If the name of the desired destination is unknown, the node cannot trigger a name resolution process. Rather, it could bypass name resolution and directly use a node's address or it could try to find a node by service discovery, but this is not part of our work.

If an application, like a web browser, wants to contact another node in our proactive routing mode, the route to the destination is available immediately without any latency for route finding if the network address of the destination node is known. However, the problem is that the route look-up cannot be done until the hostname of the destination has been translated into a network address. To avoid the latency for name resolution we use a proactive name resolution approach (cf. Figure 4).

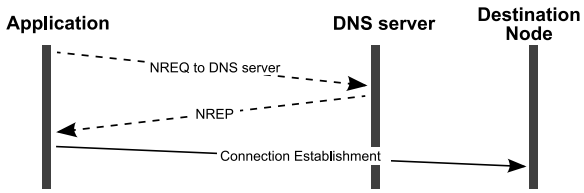


Fig. 4. Message sequence chart of connection establishment using a proactive routing protocol with and without (including the dashed lines) our extension

In proactive routing protocols, messages are periodically exchanged between the nodes. Therefore, the messages have to be small in terms of provoked traffic. For naming over proactive routing, the hostnames and network addresses have to be exchanged between the nodes, which are part of the network. A Fully-Qualified Domain Name (FQDN) [13] should have a maximum length of 255 characters containing a-z (case-insensitive), 0-9 and -. The FQDN consists of different labels with a length of 1 to 63 characters, each separated by a dot. A transmission with FQDNs directly stored inside the routing packets would let the packets grow very large and would lead to an exhaustive usage of bandwidth.

To avoid this, we calculate an MD5 hash key, which has a length of 128 bits for each hostname. This hash key is used inside the routing packets instead of the original hostname. If a

 ISBN: 978-1-61208-231-8

node searches for a specific hostname, it hashes this hostname and looks it up in the Hostname-Address-Mapping (HAM) (cf. Section III-C) table. In this way, each transmitted 'hostname' has a length of 128 bits, which is the same as an IPv6 address, instead of a maximum of $255 * 8\,\text{bits}\ (1\,\text{character}) = 2040\,\text{bits}$ (each character should be represented by 8 bits [13]). If a node wants to advertise its hostname in the proactive network, it decides whether to use the real hostname or the hash key, depending on which value is shorter or otherwise preferred by the node. In this way, each transmitted hostname has a maximum length of 128 bits, except after a COLERR message (cf. Section III-D2).

To detect hash collisions between different hostnames, each node has to check its database for identical hash keys. If a node detects a hash collision, it has to send a special Collision Error message (COLERR) inside the next OLSR routing packet throughout the network with a Time-To-Live (TTL) set to the maximum value of 255 to reach every node. Each node that receives a COLERR has to delete the corresponding hash key to address mapping inside its database and is only allowed to forward the COLERR message once to restrict flooding and to prevent exhaustive bandwidth usage. When the nodes whose hostnames corresponds to the collided hash keys will receive the COLERR, they have to send out a Name Advertisement (NADV) message containing the hostname to network address allocation. To avoid further hash key collisions these messages do not use hash keys to represent the hostname, rather they contain the hostnames in a not encrypted readable form.

As pointed out above, the usage of readable hostnames inside proactive routing messages should be avoided. For saving bandwidth we encode the single characters of the hostnames in a way that frequently used characters are represented by a shorter bit string and rarely used characters are representated by a longer bit string (c.f. 8-bit UCS Transformation Format (UTF-8) [14], which uses a similar idea). It should be noted, that processing the hostname to save bandwidth results in a higher load of a node's processor and therefore in energy usage.

If there are hostnames available that are mapped to multiple nodes, e.g., for load-balancing or multihoming, the other nodes could detect this behavior as a hash key collision. To avoid this, a hostname with multiple corresponding network addresses has to be marked in Name Advertisement (NADV) messages to notify other nodes about this circumstance. Therefore, if a node is a member of such a composition with one hostname and multiple network addresses, it has to set a special flag in its NADV messages.

If a node wants to connect to another node outside the local MANET, the node first tries to find a mapping in its HAM table. If there is no matching entry, the node forwards the request inside a conventional DNS request to one or more of the gateway nodes, which are connected to other networks.

To minimize additional packet overhead for name resolution we use the fact that mappings between hostnames and network addresses change rarely compared to the changes in routes between the nodes. Based on this behavior, the nodes exchange routing messages more often than NADV messages.

C. Hostname-Address-Mapping table

For storage of hostname to address mappings we use our new introduced Hostname-Address-Mapping (HAM) table. Each node has one HAM table that is independent from the routing protocol. Each entry in the table represents the mapping between one hostname and one network address (cf. Figure 5). If one hostname corresponds to multiple network addresses (e.g., load-balancing) or if one network address corresponds to multiple hostnames (e.g., virtual hosts), the HAM table contains multiple entries to store all mappings. If a node recognizes multiple destination network addresses for a looked-up hostname, it selects the network address with the 'best' route (e.g., in terms of hop count, bandwidth, available power) to the destination. Figure 6 shows an example for a HAM table entry with a hashed hostname mapped to an IPv4 address.

The HAM table in our proactive routing mode also provides the possibility for a simple reverse lookup from network addresses to hostnames.

Field	**Value**
Hostname Type	Type of the hostname: 0=hash key, 1=hostname
Hostname Length	Length in octets (bytes)
Hostname Value	The hostnames value either in readable form or as hash key
Address Type	Type of the network address: 0=IPv4, 1=IPv6
Address Length	Length of the network address in bytes
Address Value	The node address as IPv4 or IPv6
Flag Multihomed	This flag signalizes if this hostname corresponds to multiple network addresses
Flag Gateway	This flag signalizes if this network address belongs to a gateway node

Fig. 5. Structure of one entry in the HAM table

Field	**Value**
Hostname Type	0
Hostname Length	16
Hostname Value	e3198adf5c74a66165a458045960d51e
Address Type	0
Address Length	4
Address Value	10.1.1.3
Flag Multihomed	0
Flag Gateway	0

Fig. 6. Example of an entry in the HAM table

 ISBN: 978-1-61208-231-8

D. The Packet Types for Proactive Name Resolution

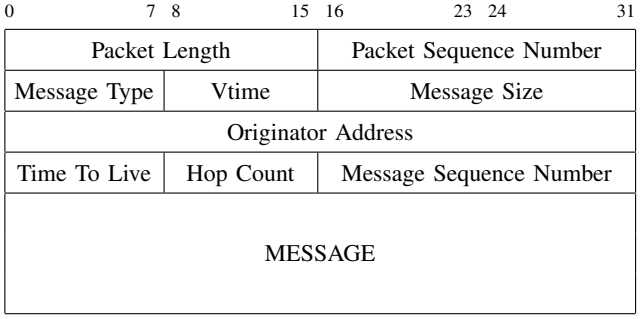


Fig. 7. Structure of OLSR messages [4]

In the reactive operation mode, our adaptive routing will use AODV as routing protocol and a name resolution mechanism similar to the approach of Engelstad et al. [2]. We do not only take the NREQ and NREP packets piggybacked with the routing messages but really integrate them inside the algorithm. So, there are two new AODV messages with included name requests and responses.

In the proactive mode, our approach will use OLSR for routing and two additional OLSR messages for name resolution. Of course, our adaptive routing framework supports also other routing protocols, but for simulation and demonstration we use AODV and OLSR.

The OLSR protocol transmits routing packages containing different messages efficiently between the nodes via Multipoint Relays (MPRs) [4]. The common structure of such routing messages (cf. Figure 7) contains a standardized header and the message body. To advertise hostname information, our proactive name resolution approach uses two additional message types, which are identified by 'Message Type' 128 for Name Advertisement (NADV) messages and 129 for Collision Error (COLERR) messages. The payload of these two introduced messages is transmitted inside the message body of the OLSR packets. The standardized header part of these messages is untouched to keep compatibility to nodes that do not support our new name resolution. The body structure of the new message types is shown in Figure 8.

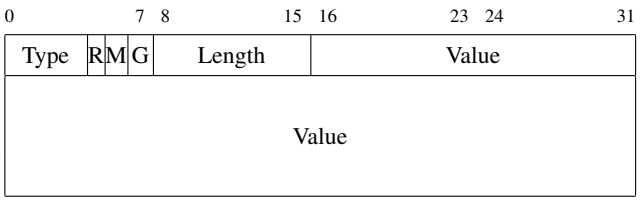


Fig. 8. Body structure of NADV messages

1) Name Advertisement Message: For hostname advertising the nodes use a Type-Length-Value (TLV) message structure (cf. Figure 8). The type field denotes the type of the hostname (0 = hash key, 1 = hostname). The 'R' bit is reserved for an extension in the future. The 'M' flag is set to a value of '1' to signalize that the following hash key or hostname is part of a multihomed system with one hostname and multiple corresponding network addresses (e.g., a load-balanced system). The 'G' flag is set to signalize a gateway node with at least one additional network interface to other networks. If this flag is set, the node can be used from other nodes as gateway to connect to networks outside the local MANET. The length field shows how many octets (bytes) are used for the following hostname. The length field has always a value of 16 if the type field is set to zero and hence signalizes an MD5 hashed hostname.

The network address of the originator of the NADV message is not stored in the message body, because it is already available in the 'Originator Address' field of an OLSR message header (cf. Figure 7). If a node uses multiple network interfaces and therefore multiple network addresses, the other nodes receive information about such addresses via 'Multiple Interface Declaration' (MID) messages of OLSR [4].

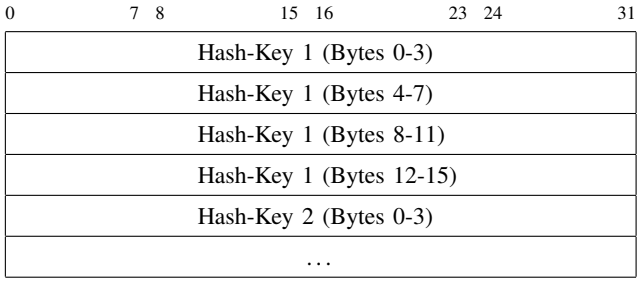


Fig. 9. Body structure of COLERR messages

2) Collision Error Message: If a node detects a hash key collision in its HAM table, it sends out a COLERR message (cf. Figure 9) with a list of all colliding hash keys. The message is broadcast throughout the whole network and all receiving nodes have to analyze such a message and to delete all corresponding hash keys in their HAM tables.

E. Transparency to the Applications

The name resolution mechanism presented in this paper has to be transparent to the applications. Therefore, all DNS requests from the application layer have to be caught, analyzed and if necessary answered by our network layer. The application should not recognize that the name resolution system has changed. Our name resolution design has the advantage that nodes that do not support the new name resolution system are still able to use conventional DNS requests and replies if there is a DNS server available in the network, which can handle the requests. This is especially important for nodes that are unaware of our new name resolution approach. Our network layer will catch such DNS requests and answer them if possible. If answering is impossible, the DNS request will be forwarded to a DNS server. If a node is aware of our new name resolution system, it can either send DNS requests, which are answered by our network layer or it could use an Application Programming Interface (API) to look directly into the HAM table to increase the performance.

 ISBN: 978-1-61208-231-8

F. Name Resolution over External Networks

Our approach is designed for usage in MANETs, where most data transmissions are limited to the MANET itself and therefore they need no special consideration. For transmissions between a node inside the MANET and a node outside the local MANET (e.g., a DNS request to the Internet), we provide name resolution over external networks.

In our system, we assume that multihomed nodes act as gateways to other networks. These networks could be other ad hoc networks or an infrastructure network with access to the Internet. Unmanned Aerial Vehicles (UAVs) with several interfaces could participate in a MANET and also be connected to a base station with Internet access at the same time. DNS requests can be forwarded to the conventional Domain Name Servers in the Internet.

In reactive networks, requests are broadcast through the network till one node replies. If the request reaches a gateway node, this node can ask the network it couples. To avoid network flooding over several MANETs, we introduce a gateway count in every NREQ packet. Each time a gateway forwards the packet, the gateway count is decreased. If the counter reaches zero, the packet will be dropped. If the gateway node has access to the global Internet, the NREQ messages are converted to normal DNS requests.

If proactive routing is used, the nodes periodically exchange topology information and therefore have an up-to-date routing table at each time. This means that each node has full knowledge about the network and furthermore knows all possible gateway nodes in the current subnet and can therefore send well-directed DNS requests to these gateways if the hostname resolution could not be resolved locally. A gateway node has to check, which name resolution system is used in the networks the name request is forwarded to. Then, it has to convert the request according to the corresponding system to achieve an adaption to the used mechanisms.

IV. Conclusion and Future Work

Our work introduces a framework for efficient name resolution in MANETs based on routing techniques. We used adaptive routing as base of our name resolution to have the best performance in different network scenarios for route finding and name mapping as well.

Because we enhanced the routing mechanism, we did not need an additional protocol for name resolution. This makes our system less complex.

In reactive routing mode, a node can directly search a route to another node's name. Compared to conventional MANETs in reactive operation mode, where a node firstly has to resolve the name and secondly has to find a route, this saves one step and therefore latency.

In our proactive routing mode, each node has all information about names and routes in the local MANET, and therefore, can transmit packets without requesting such information first. Compared to conventional proactive routing modes, this avoids the additional delay for name resolution.

We showed that centralized name resolution approaches cannot cope with the requirements of MANETs. Therefore, our fully-distributed approach eliminated centralized Domain Name Servers and increased the robustness of our MANET against failures.

There is no latency, if the name resolution uses proactive routing and decreased latency, if it uses the reactive mode. We did not need a separate protocol for name resolution by adapting the routing protocols.

As future work, we will extend our addressing scheme and mapping system to a service discovery mechanism. The problem of service discovery is similar to the problem of name resolution. In both cases a (service-)name exists and the system has to resolve this name to an address.

Furthermore, we will consider security aspects to prevent foreign nodes from masquerading other identities.

Acknowledgment

The authors would like to thank the administration and members of the International Graduate School on Mobile Communications (Mobicom) for their support and the German Research Foundation (DFG) for their kind funding.

References

[1] P. Mockapetris, "Domain Names - Concepts and Facilities," RFC 1034 (Standard), Internet Engineering Task Force, Nov. 1987, updated by RFCs 1101, 1183, 1348, 1876, 1982, 2065, 2181, 2308, 2535, 4033, 4034, 4035, 4343, 4035, 4592, 5936.

[2] P. Engelstad, D. Van Thanh, and T. Jonvik, "Name Resolution in Mobile Ad-Hoc Networks," in *10th International Conference on Telecommunications, 2003. ICT 2003.*, vol. 1, March 2003, pp. 388 – 392 vol.1.

[3] M. Menth, M. Hartmann, and D. Klein, "Global Locator, Local Locator, and Identifier Split (GLI-Split)," Institut für Informatik, Technical Report 470, April 2010.

[4] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," RFC 3626 (Experimental), Internet Engineering Task Force, Oct. 2003.

[5] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561 (Experimental), Internet Engineering Task Force, Jul. 2003.

[6] S. Nanda, Z. Jiang, and D. Kotz, "A Combined Routing Method for Ad Hoc Wireless Networks," Dept. of Computer Science, Dartmouth College, Tech. Rep. TR2009-641, February 2009.

[7] J. Hoebeke, I. Moerman, B. Dhoedt, and P. Demeester, "Adaptive Multimode Routing in Mobile Ad Hoc Networks," in *PWC'04*, 2004, pp. 107–117.

[8] N. Beijar, "Zone Routing Protocol (ZRP)," *Networking Laboratory Helsinki University of Technology Finland*, vol. 9, no. 4, pp. 427–438, 2001.

[9] O. Ponomarev and A. Gurtov, "Using DNS as an Access Protocol for Mapping Identifiers to Locators," in *Proc. of Workshop on Routing in Next Generation*, December 2007.

[10] S. Ahn and Y. Lim, "A Modified Centralized DNS Approach for the Dynamic MANET Environment," in *9th International Symposium on Communications and Information Technology*, Sept. 2009, pp. 1506 – 1510.

[11] S. Cheshire and M. Krochmal, "Multicast DNS (IETF Internet-Draft)," Feb 2011, expires: 18 August 2011.

[12] P. Engelstad, D. Thanh, and G. Egeland, "Name Resolution in On-Demand MANETs and over External IP Networks," in *IEEE International Conference on Communications (ICC '03)*, vol. 2, May 2003, pp. 1024 – 1032.

[13] R. Braden, "Requirements for Internet Hosts - Application and Support," RFC 1123 (Standard), Internet Engineering Task Force, Oct. 1989, updated by RFCs 1349, 2181, 5321, 5966.

[14] F. Yergeau, "UTF-8, a Transformation Format of ISO 10646," RFC3629 (Standard), November 2003.

 ISBN: 978-1-61208-231-8

A Middleware Architecture for Autonomic Software Deployment

Mohammed El Amine Matougui and Sebastien Leriche
Institut Telecom ; Telecom SudParis
UMR 5157 CNRS SAMOVAR,
F-91011 Evry Cedex, France
Email: {mohammed_el_amine.matougui, sebastien.leriche}@it-sudparis.eu

***Abstract*—Autonomic software deployment in open networked environments such as mobile and ad hoc networks is an open issue. Some solutions to software deployment exist; but, they are usable only within static topologies of devices. We propose a middleware architecture providing a constraint-based language guiding the deployment process at a high level and an autonomous agent-based system for establishing and maintaining a software deployment according to a deployment plan. Constraints solver generates the deployment plan from the initial specification and a network discovery service is used to automatically detect the target hosts. This paper presents middleware architecture that considers the challenges of deploying distributed software over mobile and ad hoc networks with minimal human oversight. We also present an implementation of a prototype and provide experimental results in both real environments.**

***Keywords-autonomic deployment*; *ubiquitous computing*; *mobile agents*; *middleware*.**

I. INTRODUCTION

Software deployment is defined as a complex process that includes a number of inter-related activities. Currently, there is no consensus around deployment activities. The deployment life cycle includes all activities between the software release and the software removal from deployment sites [1]. A generic deployment process covers the installation of software into the execution environment and the activation of the software, it also contains some post installation activities such as deactivation, updating, monitoring, reconfiguring (adapting) and uninstalling of the software [2].

Several large-scale deployment platforms exist, such as Software Dock [3], DeployWare [4], D&C [5], JADE [6] or more recently KALIMUCHO [7]. These deployment tools are beginning to reach their limits; they use techniques that do not suit the complexity of the issues encountered in ubiquitous infrastructures. Instead, they are only valid within fixed network topology and do not take into account neither QoS variations, nor the machine or links failures characterizing these environments. In addition, users of these deployment tools are required to manage manually the deployment activities, which represent a very significant human intervention in the deployment process. Indeed, for large distributed component-based applications with many constraints and requirements, it is hard to accomplish the deployment process manually. Clearly, there is a need for new infrastructures and techniques that automate the deployment process and offer dynamic reconfiguration of software systems with a minimum of human intervention.

To address these issues, we propose in this paper a new middleware for autonomic software deployment that is composed of (1) a domain-specific constraint language and a constraint solver for expressing deployment constraints and planning how the software will be deployed onto the target hosts (calculating a deployment plan), (2) a network discovery service and a bootstrap for the discovery of the deployment target hosts, (3) a deployment support for executing the deployment activities, and (4) an adaptable mobile agent system that runs and supervises the deployment process.

This paper is organized as follows: Section 2 introduces a motivating example and discusses the need for autonomic software deployment and the requirements of ubiquitous and mobile or ad-hoc environments. Section 3 presents an overview of our approach for autonomic software deployment. In Section 4, we present the technologies involved in our prototype and experimental results. In Section 5, we discuss some related work. Finally, in Section 6, we conclude the paper and give an overview of our future work.

II. MOTIVATING EXAMPLE

In order to highlight specificities and problems encountered for software deployment in mobile and ad hoc networks infrastructures, we present a deployment scenario, in which we deploy an activity as a monitoring application for a set of hosts (unknown at the design time) connected to a wireless network.

We consider a distributed software for providing statistical information on all hosts connected to the local area network (WiFi network). The context information in this experiment are respectively available memory size, OS type, processors usage and available disk space in each deployment target host.

At the beginning of the deployment process, the number of participants in this experiment is unpredictable; it can range from a dozen to a hundred of participants. Hosts involved in the deployment process are equipped with various hardware and software environments ranging from personal

 ISBN: 978-1-61208-231-8

computer and smartphone to ultra-mobile devices such as tablets or Personal Digital Assistant (PDA).

Each host connected to the wireless network is a potential deployment target host. The software to deploy is composed of eight components, each component being a deployment unit. The `Display-Results` component, allows the display of the statistical information computed during this experiment. This component must run on a Linux platform, and requires 40MB of RAM and at least 20% of the CPU. The components `Average-Memory`, `Average-Disk` and `Average-CPU-Occupation` calculate respectively the average of the available memory, the average disk space available and the average occupation rate of processors.

The desired deployment plan for this application is as follows: one Linux host with enough memory and CPU will get all the components. Each of the other available host will get only the components (`OS-Type`, `RAM-Size`, `Disk-Size` and `CPU-Occupation`).

To run this plan, the deployment system must face into many problems and specificities. First the discovery of available hosts in the target environment by a network discovery service. We need this step because in this 'unpredictable topology' scenario, we do not know in advance (at the design time) the list of involved hosts of the deployment process; second, there is the multiple administrators problem, as well. Indeed, the deployment target environment is a set of independent hosts where each host has its own administrator. Therefore, we must obtain the access rights on each host to be able to deploy any software.

Then, the deployment system must cover all deployment activities (from installing to uninstalling the software). The installation activity includes the software dependencies solving, transferring the components on the target sites and the physical installation of the components. At this step, the deployment system must provide a mechanism for dynamic reconfiguration of the deployment process to support the failure of hosts, the disconnections and the new connections of hosts. For example, if the selected host to have the `DisplayResults` component installed has a failure (or do not have enough RAM at the deployment time), the deployment system must dynamically find another host satisfying the constraints and go on with the deployment process. From this scenario, we conclude that the deployment platform that can addresses the specificities and problems of these environments (P2P and ubiquitous) must (Rx are requirements):

- **R1**- Be able to detect, manage and access the target hosts with a minimum user interaction.
- **R2**- Be able to deal with hardware and software heterogeneity.
- **R3**- Provide a simple and intuitive language to describe the software dependencies, the software properties and the deployment constraints.
- **R4**- Be able to compute at least one deployment plan that satisfies the deployment constraints.
- **R5**- Perform the deployment activities with minimum human intervention.
- **R6**- Provide autonomic mechanisms to reconfigure the deployment process at runtime to handle variations of the topology and hosts or network failures, accordingly to the deployment constraints.
- **R7**- Be usable in large-scale infrastructures.

III. J-ASD OVERVIEW

In this section, we present j-ASD, our middleware architecture for autonomic software deployment, which addresses the above Rx requirements. The proposed architecture is shown in Figure 1.

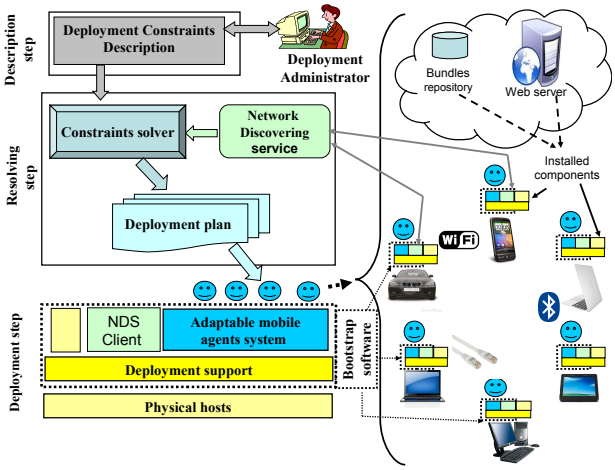


Figure 1. Architecture of j-ASD

The middleware architecture is composed of 5 different parts.

A *domain-specific constraint language* (DSL) for expressing the deployment constraints and some information on the software, a language parser and constraints solver are necessary for calculating a deployment plan.

A *network discovery service* to automatically detect target hosts in the network. By using this service, our deployment system should enable software deployment in open environments such as ubiquitous computing environments.

A *bootstrap software*, which prepares the execution environment in the target hosts of the deployment system. The bootstrap should resolve the multiple administrators problem, and install and activate all dependencies for our deployment system.

A *deployment support* equipped with a runtime environment able to run in heterogeneous infrastructures, and which can perform all or a part of the deployment activities.

Finally, we use an *adaptable mobile agent system* that performs and supervises the deployment process.

 ISBN: 978-1-61208-231-8

A. Language for Deployment Constraints

In order to automate the software deployment processes, it is necessary to have some deployment knowledge about the software system. This knowledge, is called *description of the deployment constraints*. In the existing deployment platforms, there are several formalisms to express this knowledge [3], they allow declaration of deployment constraints, software dependencies and software preferences. These methods include the use of ADL (architecture description language), the use of XML deployment descriptors (D&C [8] and CORBA [5]) and the use of a dedicated language (DSL) [9] for describing deployment constraints.

Our approach is similar to the Deladas DSL [9], discussed in the related work (Section 5). We agree with the idea of an administrator, which describes a deployment goal in terms of available resources and constraints on their deployment. But, we need much more expressiveness, particularly to deal with unpredictable aspects of the topology. For example, we want to express that one component should be deployed on each available host in the network. For this purpose, we have developed j-ASD DSL, a dedicated specific language with a simplified and intuitive syntax and grammar for describing deployment constraints.

By using the j-ASD DSL, the deployment administrator will be able to describe the software and the deployment constraints. The software is defined by a set of information about the software such as the software name, the software version, the software URL and the software components. The software is also defined by the software dependencies, the hardware and software constraints on the target hosts and finally the deployment constraints. Data types supported by j-ASD DSL are String and integer. The software can be composed of one or more components; each component is defined by the component name or ID, the component version, the component URL (the location of its implementation) and the component dependencies. Hardware and software constraints are respectively, operating system constraint `OsPref`, processor constraint `CPUPref`, memory constraint `RAMPref`, display constraint `HDPref` and network speed constraint `NetSpeedPref`. This list of constraints should be extended by adding other types of constraints and preferences like as the battery usage constraint for improving QoS offered by the j-ASD middleware.

As illustrated in Fig. 2, the deployment administrator describes a software named `ExtractFromScenario_1`, it includes two components called `ramSize` and `display`. In the same way, the component `ramSize` and `display` are defined by the component name, the component version and the component URL. The component can be located in a local repository or in a remote repository (in a web server for example). In this example, both components are located in an http server. The `hostConstraint` part is a high-level constraint specification of the display constraint on the target

```
Software {
  Name=ExtractFromScenario_1
  Version=1
  Components=ramSize display
}
Component {
  Name=ramSize
  Version=1
  Url="http://x.fr/RAM-Size.jar"
}
Component {
  Name=display
  Version=1
  Url="http://x.fr/Display.jar"
  }
  HostConstraint {
    Name=Display-Constraint
    CPULoad < 80%
    RAM >= 40 MB
    OSNameContains "Linux"
  }
  Deployment {
    ramSize @ all
    display @ 1 with Display-
    Constraint
  }
```

Figure 2. DSL code sample for Scenario 1

hosts. The `hostConstraint` name is Display-Constraint and expresses that in the deployment hosts:

- The processor constraint (`CPULoad`) in the deployment device must be less than 80%.
- The memory constraint (available memory) in the deployment device must be greater than or equal to 40 MB.
- The operating system constraint expresses that the operating system installed in the device must be Linux.

Finally, the deployment constraints are high-level constraint specifications, which express that the component `ramSize` will be deployed in each host available at the deployment time. The second constraint expresses that the component `display` will be deployed in one device that satisfies all constraints described in `Display-Constraint`.

B. Network discovery service

We use a discovery network service to allow end-users who do not necessarily know the deployment sites (devices) at the beginning of the deployment process to automatically detect these sites by invoking the service. In this context, we must distinguish two cases. The first case is the software deployment in local network (domestic network) or fixed networked devices in which the user wants to deploy the software across all (or in a subset) connected available sites in the network. The second case involves the software deployment in large-scale infrastructures like ubiquitous system and Grid. In both cases, the user does not necessarily know the deployment target host. Therefore, the deployment system must provide mechanisms to manage the network and allows the detection of each connected device in the network, then get the permissions (access rights) to each device by the bootstrap software. After the initial discovery of hosts, the network discovery service returns a host list to the deployment system. This list is used by the deployment system to produce a deployment plan.

In fixed network infrastructures, such as local area networks, several protocols such as Universal Plug-and-Play (UPnP) [10] and bonjour [11] have been successful solutions. However, these protocols do not operate effectively in

 ISBN: 978-1-61208-231-8

large-scale environments. For these, further specific discovery protocols have been created to specific domain like SLP [12], SIP [13] and XMPP [14]. For reducing interpretability issues, we have studied and chosen the UPnP and XMPP protocols to build our discovery network service. The UPnP protocols are used to deal with the first case of discovering (local network discovery) and a some parts of XMPP protocols are used to deal with the second case (large-scale network discovery) as discussed later in Section 4.

C. Bootstrap

As seen in the motivating example (Section 2), we need to deal with the multiple administrators problem. We do not want to bypass the principles of security in distributed systems, thus we must rely on each administrator to get the rights for running our deployment environment on each device. This could be achieved through a dedicated program voluntarily installed by the host administrator, and placed at its disposal through other ways. For example, it can be pushed on Bluetooth, or its url can be sent via e-mail, SMS or even embedded into a QR Code®. This very light bootstrap code is a script that asks the user the access rights to the host (such as permissions in a trusted architecture) and sets up the required runtime for the middleware.

D. Constraints solver

Once the user has completed the constraints description, the deployment system takes as inputs the constraints description program. The network discovery service is launched for detecting initial target hosts. The network discovery service returns a list of available hosts and some information about the context and resources of each one.

After syntax and lexical checking of the j-ASD DSL program, the constraints solver try to compute an initial deployment plan. For this, the program is compiled into a lower-level constraint satisfaction problem (CSP), which can be solved by a constraint solver like as JSolver [15] and Choco [16]. A CSP is expressed by declaring a set of variables whose values are drawn from a set of discrete domains, satisfying a set of given constraints. A lower-level constraint is simply a logical relation among several unknowns (or variables), each taking a value in a given domain. The constraints transformation is required because the wide gap between the level of abstraction used to model CSP programs and the abstractions used by a deployment administrator to express deployment constraints in j-ASD DSL. Our CSP problem is modeled by constructing a set of integer variables (location variables) and constraints on those variables. We model the CSP program as follow:

1) A finite set C of software components.
2) A finite set H of target devices (hosts).
3) A finite set of location variables (loc) such as:
   loc (Ci, Hj) = 1, if the software component Ci can be installed in the device Hj and loc (Ci, Hj) = 0, if the component Ci can not be installed in Hj.
4) A set P of host constraints (e.g., CPULoad and the available memory).
5) A set of deployment constraints over the location variables (loc (Ci, Hj)).

The CSP problem that we must solve in order to build an initial deployment plan is the problem of component placement on the detected device in the network in accordance with the deployment constraints.

For example, the deployment constraints described in Fig. 2 are translated as follows:

The first constraint means that the component ramSize should be deployed in all available devices, which means formally:

$ramSize \in C, \forall Hj \in H$, loc (ramSize, Hj) = 1

The second constraint means that the component display should be deployed in one device that respecting all constraints defined in Display-Constraint. This means formally:

$display \in C$, $Hi \in H$, such as: **if** $((RAM \geqslant 40MB)$ and $(OSName = "Linux")$ and $(CPULoad < 80\%)$ **then** loc (display, Hi) = 1 **else** loc (display, Hj) = 0

By using this formal translation and other (not mentioned here) we automatically generate a CSP program. Then in the second step the generated CSP program is dynamically loaded into the solving tool. The solver is then invoked to resolve the generated CSP problem and returns the first solution found. The result of solving of the generated CSP program is a set of integer and boolean variables, which are mapped as a deployment plan by the mobiles agents system. The deployment plan determines where different components of the software will be installed and executed in the target environment. If the solver cannot find a consistent solution, the constraints solver will be restarted with a new hosts list to try to find another deployment plan. If the constraints solver still unable to find a consistent solution, a failure is notified to the deployment administrator.

E. Deployment support

The deployment support should provide an execution environment and support services for components. It should allow installing, uninstalling, starting, stopping, and updating the components at runtime without restarting the entire system. It should also allow the system to deploy software on several heterogeneous devices like personal computer, laptop, PDA, tablet, smartphone, mobile phone, cars and ultra-mobile PC. Several frameworks and platforms such, as OSGi [17] or D&C [8], provide a part or all desired functionalities (life cycle deployment activities). For our prototype, we choose the OSGi platform to deploy Java-based components, as discussed later in Section 4.

 ISBN: 978-1-61208-231-8

F. Mobile Agent system

The use of mobile agents to perform an autonomic deployment process in large-scale infrastructures is not a new approach. Some works have used this technique for deploying software in static environment (for example, [3]), but they have never used this technique in ubiquitous and P2P environments.

A software agent can be defined as a program that works on behalf of its owner [18]. It is an autonomous computing entity with private knowledge and behavior. A mobile agent is a software program able to move at runtime with its code, data, and computational state [19]. An adaptable mobile agent (AMA) [20] can change some of its operating and functional mechanisms at runtime. The agent itself controls mobility and adaptation. In order to fit wide-area networks, agents communicate in asynchronous mode. A Mobile Agent System is defined as a computational framework that implements the mobile agent paradigm [21]. This framework provides services and primitives that help in the implementation, communication, and migration of software agents.

We use an adaptable mobile agent system that runs and supervises the deployment process. For this purpose, we have created the deployment agents and the supervisor agents (global and local supervisor agents).

The Supervisor agents role is performing and controlling the deployment process, it can also reconfigure the deployed software in order to react to the environment changes (host or link failures for example) in which the software is installed. Our answer to scalability issues is to have two kinds of supervisor agents: the global supervisor agent (GSA) and the local supervisor agent (LSA). There is only one global supervisor agent in our system, running initially on the host where the deployment process has been started. This agent can decide itself to move if required by the changing environment. Local Supervisor Agent is deployed by the GSA on one host for each local sub-network for scalability reasons. The LSA role is to create the deployment agents into each device in the sub-network for installing, uninstalling, activating, deactivating and updating the software and supervise the deployment process in each target host. The LSA have the ability to migrate to another host without consulting the GSA if the LSA detect a local failure (network link failure for example). This gives the opportunity for a dynamic reconfiguration of the deployment process at runtime.

The global supervisor agent (GSA) is created at the beginning of the deployment process. It performs the initial deployment plan calculated by the constraints solver. It controls the deployment process by creating local supervisor agents and then coordinating with. GSA exchange asynchronous messages with the LSA to know the status of deployment activities. Global supervisor agent provides some user interfaces to the deployment administrator. These interfaces allow users to check at any time the deployment process status and enables interventions in the deployment process at the request of the user.

A deployment agent is responsible for executing the deployment activities. Deployment agents are created and started by supervisor agents (local or global) in all target deployment devices. They perform multiple operations such as: downloading the software packages (from a web server located in a cloud computing for example) into the target devices, resolving software dependencies, installing the software in the target hosts and notify the end of the install activity by an asynchronous message. The deployment agents allow starting the installed software at the request of the supervisor agents (local or global). It can also stop all or a part of deployed software and allows the software update and uninstall on the request of the supervisor agent or the end-user request by the GUI. After installing the software, each deployment agent checks locally the correctness of the installation process and sends a message of success or failure of the installation activity to the local supervisor agent. Once the message is received, the local supervisor agent notifies the information to the global supervisor agent by sending a successful or a failure installation message.

The GSA sends an activation message for all LSA once it has received all messages of successful installation. Then, the LSA behavior is creating and sending an activation message to the deployment agents in the sub-network. If GSA has not received any messages from an LSA, the GSA considers that there is a failure; it sends a deactivation message to each LSA and a suicide message to the LSA that does not respond. The next step is creating a new local supervisor agent in another chosen host to replace LSA that not responding then restarting all stopped LSA.

IV. PROTOTYPE

To show the feasibility of our approach, we have developed a fully working prototype. Deployment constraints are expressed with our own DSL, called j-ASD DSL. It has been designed with the Xtext [22] Eclipse plugin, giving us an environment (plugins) inside the Eclipse platform to drive our middleware. The plugin uses CHOCO [16], an open source Java library for solving constraint satisfaction problems (CSP), to build the initial deployment plan. The j-ASD DSL is compiled into a single lower-level constraint satisfaction problem (Choco program), which is then solved by Choco. The generated solution is a set of integer and Boolean variables, which are mapped as a deployment plan by the mobile agent system.

We have chosen the JavAct [23] framework as a mobile agent platform [24], the OSGi Framework as a deployment support, UPnP and XMPP to discover available hosts (local and large-scale form).

 ISBN: 978-1-61208-231-8

The OSGi [17] specification comprises a framework that provides an execution platform for Java-based components, called bundles. A bundle is the physical unit of deployment. Concretely, a bundle is a Java JAR file that contains a manifest and some combination of Java class files, native code, and any associated resources. OSGi allows installing, uninstalling, starting, stopping, and updating bundles at runtime without restarting the entire system and includes a generic mechanism for automatic dependencies management. Using OSGi as a deployment support allows us to deploy software on several heterogeneous infrastructures. The reuse of the deployment activities provided by the OSGi framework like installing and uninstalling bundles allows us to focus on other aspects of the deployment process. Currently, our deployment units are OSGi bundles. Deployment of other deployment units will be envisaged later. We use the OSGi Framework Equinox [25].

We have also developed mobile agents behaviors and algorithms for installing, starting, stopping, uninstalling and updating the deployment units. The current implementation allows the deployment of applications composed by one or more OSGi bundles on the OSGi runtime environments. The prototype allows us to create and send our specialized mobile agents to the targeted hosts in the network, to execute and supervise the deployment activities in the most installable environment like ubiquitous systems. These agents give us the possibility of reconfiguration and dynamic adaptation to the execution context of the deployed software. An example of adaptation is the decision to migrate to another target device if the current one does not have enough resources like memory or bandwidth.

In addition, we have built a network service for the discovery of the target hosts. We wanted some open sources/protocol technologies, to reduce interoperability issues. We found that UPnP [10], the XMPP [14] protocol, the SIP [13] protocol, or the SLP [12] protocol could be a basis for our discovery network service. At the end, we chose the UPnP [10] and XMPP [14] protocols with the Cyberlink [26] and Smack [27] open-source implementations integrated behind a lightweight facade design pattern. The XMPP and SIP protocols address multimedia session management and presence signalization. The idea is to use the UPnP technology for discovering target hosts in local networks (LAN), and the XMPP protocol for discovering the deployment hosts within a large-scale deployment (WAN).

At the time of writing, the prototype is functional. We are now working on the experimental evaluation and the validation of the deployment process in a real environment. We conducted several tests on wired and wireless network. Each experiment was performed five times to produce the time required to compute de deployment plan, the necessary time to detect the deployment hosts and the time needed to deploy the components into the target hosts.

The first experiment we have conducted concerns the time needed for computing the initial deployment plan. The performance data was obtained on a duel core Intel Pentium III Xeon 2.4 GHz laptop with 4GB RAM running Windows XP professional edition. The time needed for computing the initial deployment plan of 20 components into 200 hosts with 20 constraints is below 1 minute. We tried 20 components into 5000 hosts with 15 constraints; computing time can be up to 20 minutes. As shown in Fig. 3, the average time needed to for computing the initial deployment plan for the presented example in Section 2, for 10 and 3200 hosts is respectively 16 and 292 milliseconds.

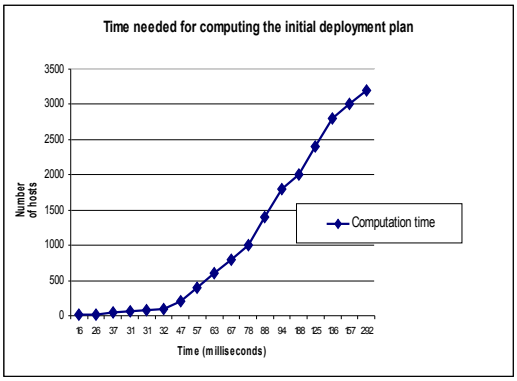


Figure 3. Time to compute the deployment plan results

The second experimentations series concerns the average time of discovering the devices and the average installation time. The install activity includes, the mobile agent creation, the bundles downloading in the target hosts, the bundles installation and the notification of the success of the bundle installation. This experimentation has been conducted on a fully connected 100 Mb/s Ethernet network of workstations (Intel(R) Xeon(R), 2.80GHz, 4029MB) and WiFi network of Samsung PC tablets (Intel(R) processor 800MHz, 0,99GB). The time needed to detect 60 devices is 15 seconds in the wired network and 16 seconds to detect 10 devices connected in the Wireless network.

As depicted in Fig. 4, the average installation time for the software presented in Section 2 (software composed from eight components) in 60 hosts is less than 13 seconds. For more details, you can download the full results of experiments (in French) from [28].

V. Related work

There are typically many constraints in the deployment of large-scale applications into distributed environments. For this purpose, software deployment process is given special attention both in academia and in industry and there is a large number of tools, procedures, techniques, and papers addressing different aspects of the software deployment process from different perspectives. In this section, we

 ISBN: 978-1-61208-231-8

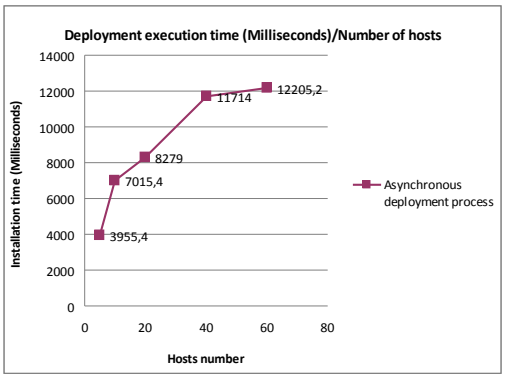


Figure 4. Installation time results

present some of the research literature related to software deployment.

Fractal Deployment Framework (FDF) [4] is a component-based software framework to facilitate the deployment of distributed applications on networked systems. FDF is composed of a high-level deployment description language, a library of deployment components, and a set of end-user tools. The high level FDF deployment description language allows end-users to describe their deployment configurations (the list of software to deploy and the target hosts). The main limitation of this tool is the static and manual attributes of the deployment. Although the static deployment plan is eligible in stable environment like Grid, this deployment is not usable in an environment characterized by a dynamic network topology like ubiquitous environments. Another limitation is that, at runtime this tool does not provide mechanisms for dynamic reconfiguration, which allows the treatment of the hosts and the network failures.

The Software Dock [3] is a research project, which provides a framework for software configuration and deployment. It has created a distributed, agent-based deployment framework, which supports cooperation among software producers themselves and between software producers and software consumers. The deployment framework uses client-server architecture in combination with an event system. However, Software Dock does not allow the description of the software architecture and propose a static centralized deployment process, which does not suit our requirements of dynamic adaptation and scalability.

R-OSGi [29] is a middleware platform that extends the standard OSGi specification to support distributed module management. R-OSGi provides a deployment tool to help developers to distribute an application by dragging and dropping between a visualization of the modules of the application and a representation of the distributed node available. The developer of R-OSGi application has full control on how the application is distributed. Creating a configuration and controlling the deployment process in the context of large-scale systems is a complicated task, which represent for us a heavy human intervention in the deployment activities. In addition, R-OSGi is only intended to create static deployments and cannot be used within open environments that are characterized by dynamic network topology such as shown in our scenario.

Dearle et al. [9], [30] propose a middleware framework for deployment and subsequent autonomic management of component-based applications. The deployment constraints of distributed applications are specified using the Deladas (DEclarative LAnguage for Describing Autonomic Systems) language. An initial deployment goal is specified by using the Deladas language, and then, in order to produce a concrete deployment of the application, the automatic deployment and management engine ADME attempts to generate a configuration that describes which components are deployed in which nodes by using a constraints solver. This approach has the similar motivations to our approach; in fact, one of the motivations is the costs reduction involved in human-managed system maintenance by the automatic generation of the deployment plan and with the mechanisms for reconfiguring the deployment at runtime. However, this centralized solution can not work in a change-prone environment (unpredictable topology), and needs a full restart of the deployment process for each error found at runtime. Our solution, involving decentralized decisions of deployment adaptation by mobile agents which allows to make light and local reconfiguration that are realistic (and scalable) in large scale and error-prone topologies.

VI. Conclusion and Future Work

Our contribution in this paper can be summarized as follows. We described a scenario where other software deployment tools will fail; we discussed the need for autonomic software deployment in large-scale and change-prone infrastructures (Ubiquitous systems, P2P systems) and the requirements for such a platform. We presented j-ASD, our middleware dedicated to autonomic software deployment, and some elements of the prototype that validate our approach.

The j-ASD middleware addresses the requirements and specificities of those environments. (1) We have chosen the OSGi Framework as a deployment support to allow Java-based components deployment on several types of heterogeneous hardware. (2) The network discovery system and the bootstrap software allow the management and the access to the target devices with a minimum user interaction. (3) j-ASD DSL is an intuitive and a declarative way to specifies the deployment constraints (high-level constraints), the j-ASD DSL is compiled into a lower-level constraint satisfaction problem (CSP), which are resolved automatically by Choco solver. (4) The generated solution is dynamically mapped as an initial deployment plan by the mobile agents

 ISBN: 978-1-61208-231-8

system. (5) Thanks to the characteristics of mobile agents (autonomous behavior and ability to migrate), we can perform adaptations and dynamic reconfigurations at runtime without any user intervention.

We are currently pursuing our work on the evaluation of the last version of the j-ASD prototype toward large scale distributed systems and investigating on smarter algorithms to deal with the need for adaptation in more complex failure situations after the initial deployment.

REFERENCES

[1] A. Dearle, "Software deployment, past, present and future," in *FOSE*, 2007, pp. 269–284.

[2] A. Carzaniga, A. Fuggetta, R. S. Hall, D. Heimbigner, A. van der Hoek, and A. L. Wolf, "A characterization framework for software deployment technologies," Dept. of Computer Science, University of Colorado, Tech. Rep., 1998.

[3] R. S. Hall, D. Heimbigner, and A. L. Wolf, "A cooperative approach to support software deployment using the software dock," in *Proceedings of the 21st international conference on Software engineering*, ser. ICSE '99. ACM, 1999, pp. 174–183.

[4] A. Flissi, J. Dubus, N. Dolet, and P. Merle, "Deploying on the grid with deployware," in *CCGRID*, 2008, pp. 177–184.

[5] O. M. Group, "Corba component model 4.0 specification," Object Management Group, Specification Version 4.0, April 2006. [Online]. Available: http://www.omg.org/docs/formal/06-04-01.pdf

[6] C. Taton, S. Bouchenak, N. De Palma, D. Hagimont, and S. Sicard, "Self-sizing of clustered databases," in *WOWMOM '06*, 2006, pp. 506–512.

[7] C. Louberry, P. Roose, and M. Dalmau, "Kalimucho: Contextual Deployment for QoS Management," in *11th IFIP WG 6.1 International Conference, DAIS 2011, Reykjavik, Iceland, June 2011, Proceedings*, vol. 6723, Jun 2011, pp. pp.43–56.

[8] OMG, "Deployment and configuration adopted submission, document ptc/03-07-08 ed." Object Management Group, Tech. Rep., July 2003.

[9] A. Dearle, G. N. C. Kirby, and A. McCarthy, "A framework for constraint-based deployment and autonomic management of distributed applications," *CoRR*, vol. abs/1006.4572, 2010.

[10] UPnP Forum, "UPnP Device Architecture, V 1.1," October 2008. [Online]. Available: http://www.upnp.org/

[11] APPLE, "Bonjour protocol specifications." March 15 2011. [Online]. Available: http://developer.apple.com/networking/bonjour/specs.html

[12] E. Guttman, "Service location protocol: Automatic discovery of ip network services," *IEEE Internet Computing*, 1999.

[13] R. Sparks, "Sip: Basics and beyond," *Queue*, pp. 22–33, March 2007.

[14] P. Saint-Andre, K. Smith, and R. Tronçon, *XMPP: The Definitive Guide: Building Real-Time Applications with Jabber Technologies*. O'Reilly Media, Inc., 2009.

[15] A. H. W. Chun, "Constraint programming in java with jsolver," 1999.

[16] C. Team, "choco: an open source java constraint programming library," Ecole des Mines de Nantes, Research report, 2010. [Online]. Available: http://www.emn.fr/z-info/choco-solver/pdf/choco-presentation.pdf

[17] The OSGi Alliance, "OSGi service platform core specification, release 3. version 4.2," 2009.

[18] J. M. Bradshaw, Ed., *Software agents*. Cambridge, MA, USA: MIT Press, 1997.

[19] C. G. Harrison, C. G. Harrison, D. M. Chess, D. M. Chess, A. Kershenbaum, and A. Kershenbaum, "Mobile agents: Are they a good idea?" 1995.

[20] S. Leriche and J.-P. Arcangeli, "Flexible architectures of adaptive agents : the agentϕ approach," *International journal of grid computing and multi agent systems (IJGCMAS)*, pp. 55–75, 2010, 8878.

[21] R. S. S. Filho, "Mobile agents and software deployment," ICS280 Configuration Management and Runtime Change Final Paper, Information and Computer Science Department, University of California Irvine, Fall, Tech. Rep., 2000.

[22] "Xtext 2.3 Documentation," June 28 2012. [Online]. Available: http://www.eclipse.org/Xtext/documentation/2.3.0/Documentation.pdf

[23] S. R. J.-P. Arcangeli, F. Migeon, "JAVACT : a Java middleware for mobile adaptive agents," January 5 2011. [Online]. Available: http://www.javact.org

[24] J.-P. Arcangeli, C. Maurel, and F. Migeon, "An api for high-level software engineering of distributed and mobile applications," in *Distributed Computing Systems, 2001. FTDCS 2001.*, 2001.

[25] "Getting Started with Equinox," 2012. [Online]. Available: http://www.eclipse.org/equinox/

[26] "CyberLink for Java," September 9 2012. [Online]. Available: http://www.cybergarage.org/twiki/bin/view/Main/CyberLinkForJava

[27] "Smack documentation," February 5 2012. [Online]. Available: http://www.igniterealtime.org/projects/smack/

[28] Y. Wang, M. E. A. Matougui, and S. Leriche, "j-asd experiments," Institut Telecom ; Telecom SudParis, Tech. Rep., August 15 2012. [Online]. Available: http://javact.org/JASD-rapport.pdf

[29] J. S. Rellermeyer, G. Alonso, and T. Roscoe, "R-OSGi: distributed applications through software modularization," in *MIDDLEWARE2007*. Berlin, Heidelberg: Springer-Verlag, 2007.

[30] A. Dearle, G. N. C. Kirby, and A. J. McCarthy, "A framework for constraint-based deployment and autonomic management of distributed applications," in *ICAC*, 2004.

 ISBN: 978-1-61208-231-8

Improvements to Tree-based GA Applications for QoS Routing

Vincenzo Maniscalco, Silvana Greco Polito, and Antonio Intagliata

Facoltá di Ingengeria, Architettura e delle Scienze Motorie
Libera Universitá degli Studi di Enna "KORE"
Enna, Italy
{vincenzo.maniscalco,silvana.grecopolito, antonio.intagliata}@unikore.it

***Abstract*—Genetic Algorithms (GAs) are emerging as a promising instrument for quality of service (QoS) routing in Mobile Ad hoc Networks (MANETs). They implement an iterative process that can solve the NP search problem of routing with multiple QoS constraints. In each iteration new solutions are found through the mutation and crossover genetic operations. In this paper we focus on an existing GA tree-based application for QoS routing in MANETs which applies the genetic operations on a tree built from the network topology and uses fixed length chromosomes. The chromosome encodes junctions tree crossed by routes. This application suffers in convergence speed because its mutation operator does not allow deep exploration of the search space. The inefficiency of the adopted mutation operation is more evident in networks with big size and high network connectivity, i.e., networks with a larger search space. In this paper, we elaborate on the tree-based application with the main objective of improving its performance. We first introduce a criterion for junctions tree sorting based on their distance from the root. Later, we use chromosome properties due to the sorting criterion to design a sequential mutation technique with adaptive probability that allows faster convergence. We provide simulation results showing the effectiveness of the proposed enhancements while increasing the MANET size and connectivity.**

Keywords-Genetic Algorithm; QOS routing; junctions tree; MANET

I. INTRODUCTION

MANETs are composed of wireless nodes that can move, join and leave the network dynamically. They can be used in different scenarios such as campus and disaster recovery areas for communication between students or emergency operators. They do not refer to a fixed infrastructure and need routing protocols that adapt to topology changes quickly. They also need routing algorithms that can provide quality of service (QoS) routes, i.e., routes satisfying QoS constraints such as delay or jitter posed by realtime applications. Therefore the need of QoS routing for MANETs is motivating research work on QoS protocols [1], metrics and algorithms [2]. Regarding QoS algorithms, the Literature shows an increasing interest around solutions based on Genetic Algorithms which can solve NP problems. GA routing algorithms, given network topology and QoS costs of network components, implement genetic operations to search the best route subject to multiple QoS constraints. This is known to be an NP problem. The Literature discusses two main GA approaches for QoS routing with fundamental differences in their encoding schema. An approach employs variable length chromosomes with genes representing the nodes along a route from source to destination [3-5]. The other models the set of routes from source to destination as a tree and implements a coding schema with fixed length chromosomes [6-8]. Genes of the chromosome encode the junctions tree. The main advantages of the tree-based approach are due to the tree structure that avoids loops generation during the GA process, and the fixed length of the chromosome that allows to use simpler models for genetic operations.

In this paper, we elaborate on the main existing tree-based GA application for QoS routing introduced by Barolli et al. in [6-8], and we propose enhancements that strongly improve its performance. We have observed that the convergence of the existing tree-based applications becomes slower while increasing network connectivity and network size as the mutation probability, which is fixed (it is equal to the inverse of the chromosome length), does not allow deep exploration of big search space. Available results [6] describe the algorithm scalability while increasing the number of nodes in the network, but how scalability is affected by the number of links per node is not discussed. In addition tree-based chromosomes have to be sorted properly to avoid generation of invalid routes with genetic operations. Although the authors [9] are aware of this problem they do not propose a sorting model.

To overcome the above discussed lacks, we (i) introduce a proper sorting model for genes within the chromosome, and (ii) propose a sequential mutation technique with adaptive probability. The sorting model makes junctions representation within the chromosome dependent on their depth, i.e., the distance from the source. It avoids generation of invalid routes from genetic operations. The mutation technique uses a mutation probability which adapts to any specific route: it is equal to the inverse of the junctions number crossed by the route. The adaptive probability allows deeper exploration of the search space and therefore faster convergence to better QoS routes. We carry out simulations demonstrating the strong effect of the mutation solution on the scalability of the GA application while increasing both network size and node connectivity. Study of protocols for acquisition and maintaining

 ISBN: 978-1-61208-231-8

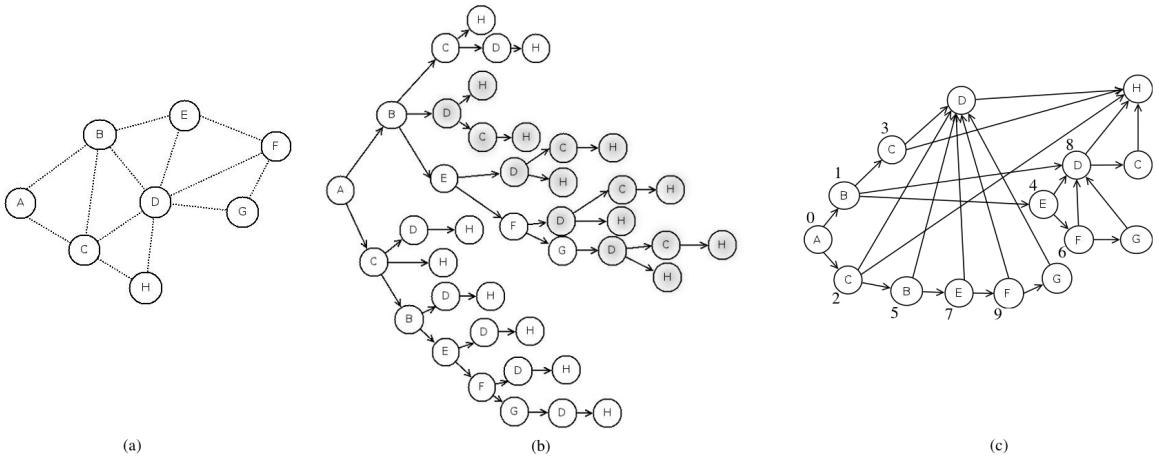


Fig. 1. (a) MANET example; (b) Tree network for source A and destination H; (c) Reduced tree network.

of topological information is out of the scope of this paper. Any protocol able to collect topology and QoS data can be used as the one discussed in [10]. According to this protocol the source sends route discovery requests in flooding toward the destination, which replays with multiple routes and per hop QoS parameters.

The remaining of the paper is organized as follows. In Section II we summarize the main aspects of the tree-based GA approach to which we refer. In Section III we introduce the criterion for junctions sorting and we describe the adaptive mutation method. Section IV provides simulation results showing the performance improvements due to the proposed enhancements while increasing network size and connectivity.

II. Review of GA and the tree-based application for QoS routing

GA is a heuristic method that simulates the natural evolution process to solve optimization problems. In the following we first introduce the GA iterative process and later we review the existing tree-based GA application for QoS routing in MANETs.

A. The GA iterative process

GA employes iterative processes on a set of individuals representing a generation for each cycle [11]. Each individual is a candidate solution and is encoded with a chromosome composed of genes. The GA process includes two main stochastic genetic operations, i.e., crossover and mutation. The former is to transmit the genetic heredity from selected parents to next generation. The parents' selection process is based on a fitness function which depends on constraints of the specific problem to solve. For selected parents, the crossover operation exchanges parts of their chromosomes to generate new descendants. These descendants are submitted to the mutation operation that changes their genes for the new generation. Usually, the GA starts with an initial population chosen at random and the cycle repeats until the solution is found or termination criteria are satisfied. Bigger population sizes guarantee solutions with better quality. The number of evaluations of the fitness function, which increases with the number of iterations and the size of the initial population, measures the GA computational complexity. When applications have stringent time constraints, fast GA hardware implementations in FPGA can be used [12].

B. The existing tree-based method for QoS routing

In the tree-based genetic algorithm for QoS routing proposed by Barolli et al. [6-9], the network (Figure1.a) is modelled as a tree having the source node as root and the destination node as leafs (Figure 1.b). The chromosome structure is expressed by the tree junctions which leads to fixed chromosome length. To compact the chromosome length a tree reduction algorithm has been proposed [9]. Tree reduction is carried out merging nodes having the same identifier (ID) and the same sub-routes. In the example of Figure 1.b the four junctions D become a single junction in the reduced tree (Figure1.c). A number is assigned to each junction which is its locus in the chromosome. Each gene can assume the value of one of the adjacent junctions. Genes may be active or inactive: a gene is active if its corresponding junction is in the route. Gene values are assigned only to active genes. In Figure 2 the gene encoding and an encoded route are shown.

0(A)	1(B)	2(C)	3(C)	4(E)	5(B)	6(F)	7(E)	8(D)	9(F)
B/C	C/D/E	B/D/H	D/H	D/F	D/E	D/G	D/F	C/H	D/G

(a)

B	E	--	--	F	--	G	--	H	--

(b)

Fig. 2. (a) Gene coding; (b) Chromosome encoding the route $A-B-E-F-G-D-H$.

Genetic operations must be carried out between active genes. In this manner, the crossover operation interchanges sub-routes in the tree network from the junction that corresponds to the crossover point, while the mutation operation

generates a new suitable sub-route from the junction that corresponds to the mutation point.

Regarding the fitness function, delay time (DT) and transmission success rate (TSR) are used to express the QoS of a route as in the following equation where N is the number of links in a route:

$$T = \frac{\sum_{i=1}^{N} DT_i}{\prod_{i=1}^{N} TSR_i} \quad (1)$$

The rank selection method is used along with single point crossover, and elitism to maintain the best solution in the next generation. The mutation technique is not discussed, the mutation probability is equal to the inverse of the chromosome length.

III. Enhancements to the tree-based GA application for QoS routing

The enhancements to the tree-based application are (a) a proper junction sorting criterion, and (b) a novel mutation technique with adaptive probability. The junction sorting criterion leads to a chromosome structure that depends on the junctions depth. This feature is used to get always valid routes from genetic operation. We also leverage on it to build the mutation technique.

A. Junction sorting

Junction sorting is based on the distance from the junction to the root, which is called junction depth. In the following we first introduce the sorting criterion and later on the main chromosome properties derived from it.

1) Depth-based sorting criterion: It consists of the following three steps.

Step 1: Build a junction tree from the tree network with junctions sorted according to their distance from the route. The sorted junctions tree for the network of Figure 1 is shown in Figure 3. In this example, the root junction A has depth equal to 0, the junctions B and C have depth 1 and so on.

Step 2: Merge junctions for tree reduction and assign the highest depth to them. For the example of Figure 3 this means assigning depth 4 to the junction D.

Step 3: Encodes the junctions within the chromosome according to their depth in the reduced junction tree.

This criterion guarantees that genetic operations always result in valid routes. How invalid routes can be created when junctions are not sorted properly is shown in the example of Figure 4. In this example, the junction D is located in the 5th gene instead of the 8th. If we perform crossover between routes A-B-E-D-C-H and A-B-D-H with crossover point D, an invalid descendent is generated as the 5th gene is inactive. If the mutation operator does not change the values of this chromosome the decoding operation does not return a route.

2) Chromosome properties due to sorting: The junction sorting criterion also leads to the following chromosome encoding properties:

- At most one gene encoding junctions with the same depth may be active.

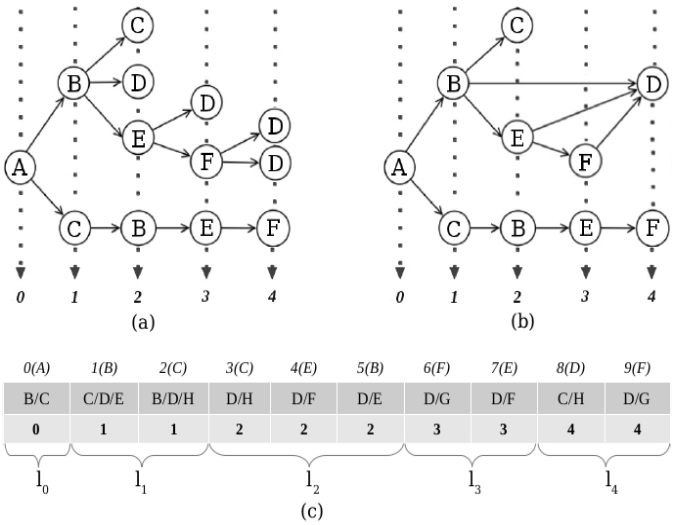


Fig. 3. (a) Junctions tree; (b) Reduced junctions tree; (c) Chromosome structure sorted by depth

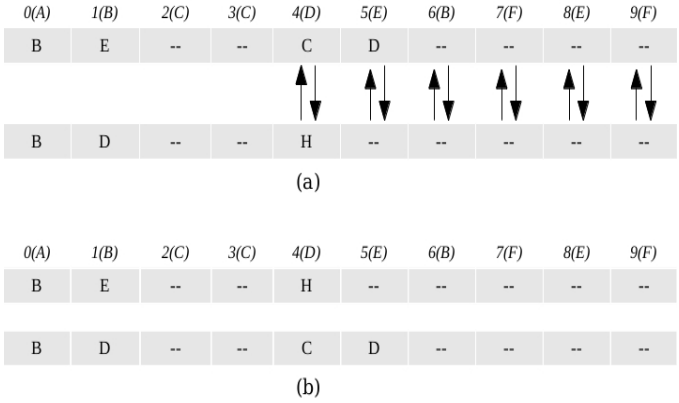


Fig. 4. (a) Single-point crossover between chromosomes sorted improperly; (b) Invalid descendants.

- If two junctions with different depths are directly connected, all the genes encoding junctions between them are inactive.
- If a gene encodes a junction reaching the destination, then all the following genes are inactive.

B. Sequential mutation technique with adaptive probability

The encoding chromosome properties due to junction sorting described in the previous section let us design a sequential mutation technique with adaptive probability. This is equal to the inverse of active genes number for each chromosome. The mutation details are the following:

(1) Apply the mutation probability to each active gene of the chromosome sequentially until a mutation point is found or the chromosome is ended;
(2) If the mutation point has been found, take into account the set of adjacent nodes, excluding the current one, and select one of them with equal probability. Deactivate the following genes in the chromosome.

 ISBN: 978-1-61208-231-8

(3) Search the chosen node in the reduced tree network;
- If this node is a junction, select one of the adjacent nodes with equal probability for the gene of the junction and return to step (3);
- If this node is not a junction and it is not the destination, take into account the next element in the tree network and return to step (3);
- If this node is the destination, the algorithm ends.

We point out that mutation is always applied once a mutation point is found and the route is always valid. If D is the highest depth level, the mutation probability range can be expressed as follows:

$$\frac{1}{D} \leq p_m \leq 1 \quad (2)$$

In other words, the mutation probability is maximum when source and destination nodes are directly connected, while it is minimum when the route that connect them crosses one junction per each depth.

IV. Performance Study and Discussion

This performance study aims to show the effects of adaptive mutation probability on the tree-based application while increasing the network size and connectivity. For this purpose, we have implemented the tree-based GA application with both the fixed mutation probability introduced in [6-9] and the adaptive mutation probability proposed in this paper. For both the implementations we have used the junction sorting criterion and the mutation technique proposed in Section III-A and Section III-B, respectively, as any description of them is missing for the existing application. Therefore, the two implementations have the same computational cost. The implementations are made with initial population generated randomly, linear ranking selection method, single point crossover and elitism. The fitness function is the one in eq (1) with DT and TSR selected randomly. Each simulation runs 1000 times and provides the rank, i.e., the position of the solutions sorted according to their fitness, as output. Simulations are carried out with MATLAB.

In the following, we will refer to the two implementations as fixed-GA and adaptive-GA, respectively.

A. Scalability while increasing the network connectivity

Figures 5 and 6 show the rank achieved by the GA application with both fixed and adaptive mutation probability on a sparse and dense network. The sparse and dense networks have 3 and 5 links per node on average, respectively. These figures also report the size of the search space (routes) and the chromosome length. Population sizes are selected equal to 20 and 50 in the sparse and dense networks, respectively.

In the sparse network (see Figure 5), the application with adaptive mutation probability convergences around the 10th generation, while the applications with fixed mutation probability converges on the 20th generation. Therefore, the adaptive mutation probability cuts by half the computation complexity, which is equal to (population size)*(iterations number). The performance improvements are stronger in the dense network as shown in Figure 6. In this scenario the application with adaptive mutation probability convergences around the 50th generation, while the native application is still far to converge. This because dense network does have big chromosome length L and the fixed mutation probability equal to $1/L$ is too small for a deep exploration of the search space.

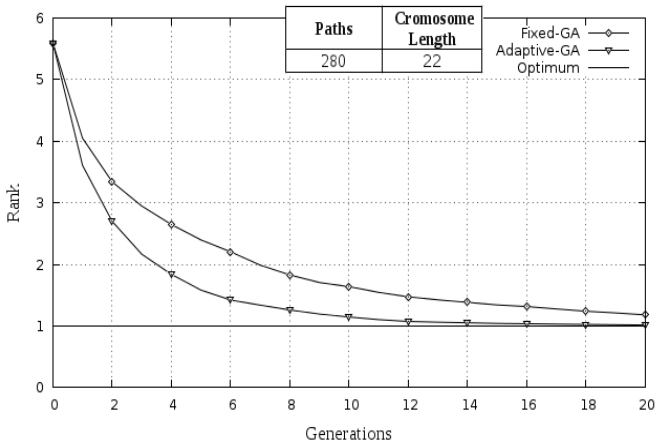


Fig. 5. Comparison between fixed-GA and adaptive-GA in sparse networks

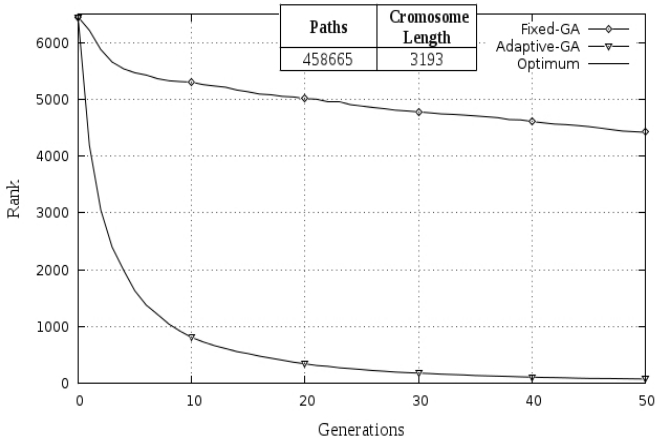


Fig. 6. Comparison between fixed-GA and adaptive-GA in dense networks

Figures 7 and 8 show the convergence curves of the GA application with adaptive mutation for different population sizes. We have used them to set the population size of the previous simulations. The population size of 20 guarantees convergence to the optimum solution on the 20th generation in the sparse network. The one of 50 for the dense network guarantees convergence to a suboptimal solution on the 50th generation. We recall that (see Section II-A) the population size should be selected according to the desired trade-off between computation complexity and quality of solution, which depends on the specific application and the computation features of the mobile nodes. The total computation cost and delay of any tree-based GA application also depends on the tree generation and reduction procedure which increases with

 ISBN: 978-1-61208-231-8

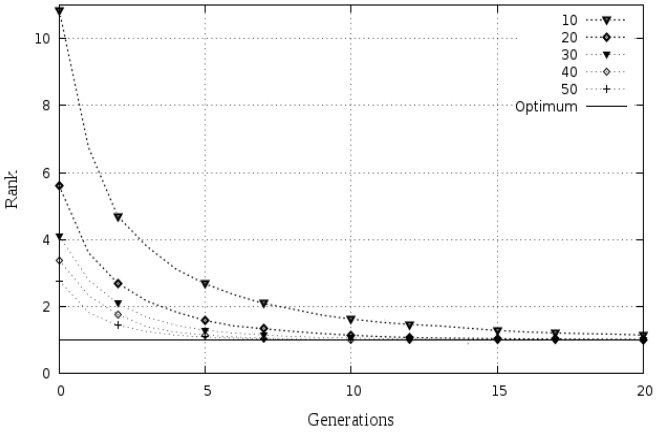


Fig. 7. Performance for different population sizes in sparse networks

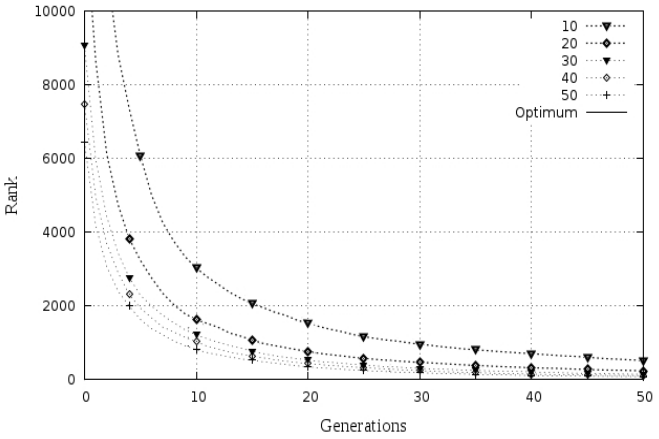


Fig. 8. Performance for different population sizes in dense networks

the solutions space. Note that it is around 458.000 for the dense network with 5 links per node. MANET scenarios with high mobility speed poses constraints on the delays for route discovery, therefore the applicability of the algorithm in high connected networks depends on the mobility speed.

B. Scalability while increasing the network size

The effects of network size on the GA application convergence is shown in Figures 9, 10 and 11 with networks of 20, 30 and 40 nodes, respectively. The connectivity density is of 3 links per node on average.Simulations are made with population size equal to the number of nodes. QoS DT/TSR parameters are selected and network topologies are generated randomly per each of the 1000 simulations. Given the population size, the total number of generations is chosen according to the convergence of the faster application, which is always the one with adaptive mutation probability.

The results in Figure 9 show that, although the implementation with adaptive mutation probability has higher convergence speed, the behavior of the other implementation is similar as it was expected from the results in Figure 5. Improvements on performance increase in the bigger networks. In

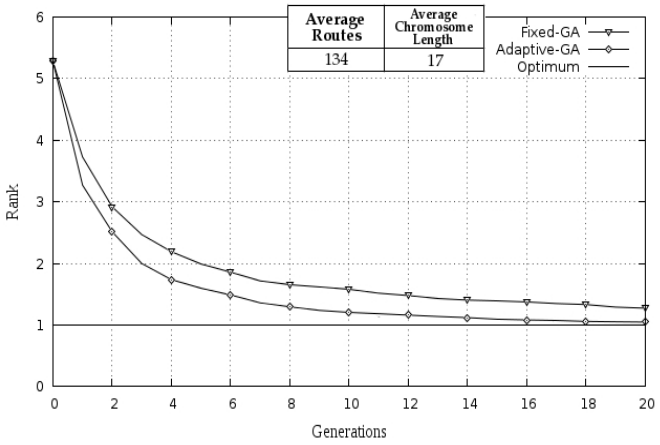


Fig. 9. Comparison between fixed-GA and adaptive-GA for a network with 20 nodes

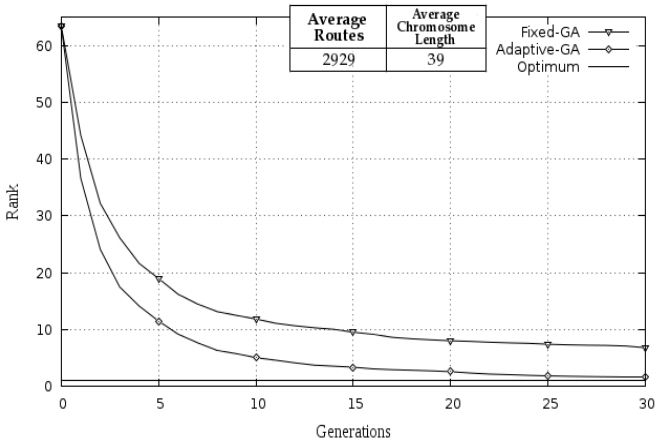


Fig. 10. Comparison between fixed-GA and adaptive-GA for a network with 30 nodes

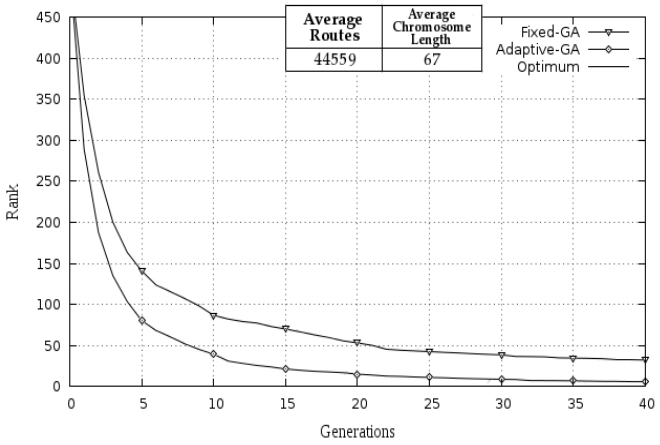


Fig. 11. Comparison between fixed-GA and adaptive-GA for a network with 40 nodes

these networks, while the applications with adaptive mutation probability converge to the optimum or a close to optimum solution, the GAs with fixed probability provide low quality solutions (see Figure 10 and 11). The reason is the same pointed out for high connected networks: bigger networks have larger search space and longer chromosome and then a fixed mutation probability does not allow deep exploration of the search space.

Note that the number of routes does not increases linearly with the number of nodes. When the search space explodes the computational cost of the tree-generation process may be prohibitive. In these networks the GA application can be used with clustering architectures to work on smaller search spaces. This is similar to what done by the authors of [13]. They divide the network in zone and apply a GA-based algorithm with variable length chromosomes for inter-zone routing. Objective of our future study is verifying how to apply the GA tree-based approach on clustering architectures.

C. Statistics for the simulation results

As statistics for the simulation results we consider the standard deviation. We report in Table I rank and standard deviation for the first results of Figure 5. Note that the standard deviation decreases while increasing the generation number. This is also true for all the other simulations.

TABLE I
STANDARD DEVIATIONS FOR RESULTS IN FIGURE 5

Generations	Fixed-GA		Adaptive-GA	
	Rank	Standard Deviation	Rank	Standard Deviation
12	1,54	1,19	1,10	0,40
14	1,42	1,03	1,06	0,32
16	1,34	0,92	1,04	0,26
18	1,27	0,84	1,03	0,24
20	1,21	0,74	1,02	0,19

V. CONCLUSION AND FUTURE WORK

In this paper, we have proposed enhancements to the existing tree-based GA application for QoS routing in MANETs. We have discussed how the fixed mutation probability adopted for this application does not allow a deep exploration of the search space and therefore leads to slow convergence or convergence to solutions with low QoS. We have introduced a criterion for junction sorting based on the junction depth and we have proposed a sequential mutation technique with adaptive probability. The adaptive probability of the mutation technique allows a deeper exploration of the search space, which leads to faster convergence and better QoS solutions for given generations. We have shown with simulation results that the adaptive mutation probability strongly improve the performance of the tree-based GA application, particularly in big or highly connected networks. Future purposes will be about the application of the GA tree-based approach to clustering architectures.

REFERENCES

[1] S. Mittal, P. Kaur, *Performance Comparison of AODV, DSR and ZRP Routing Protocols in MANET'S*, International Conference on Advances in Computing, Control, and Telecommunication Technologies, Trivandrum, India, December 2009.

[2] L. Hanzo, R. Tafazolly, *A Survey of QoS Routing Solutions for Mobile Ad hoc Networks*, IEEE Communications Surveys, Vol.9, N.2, pp. 50-69, 2009.

[3] Chang Wook Ahn, R.S. Ramakrishna, *A Genetic Algorithm for Shortest Path Routing Problem and the Sizing of Populations*, IEEE Transactions on Evolutionary Computing, Vol. 6, pp. 566 - 579, December 2002.

[4] S. Yang, H. Cheng, F. Wang, *A genetic Algorithms With Immigrants and Memory Schemes for Dynamic Shortest Path Routing Problems in Mobile Ad Hoc Networks*, IEEE Transactions on Systems, MAN and Cynernetics-Part C: Applications and Review, Vol. 40, N.1, pp.52-63, January 2010.

[5] S. Yussof, O. H. See, *A Robust GA-based QoS Routing Algorithm for Solving Multi-constrained Path Problem*, Journal of Computers, Vol. 5, N.9, September 2010.

[6] A. Barolli et al., *Application of Genetic Algorithms for Qos Routing in Mobile Ad-Hoc Networks: A Survey*, International Conference on Broadband, Wireless Computing, Communication and Applications, Fukuoka, November 2010.

[7] L. Barolli, A. Koyama, N. Shiratori, *A QoS Routing Method for Ad-Hoc Networks Based on Genetic Algorithm*, 14th International Workshop on Database and Expert Systems Applications (DEXA'03), Prague, Czech Republic, September 2003.

[8] A. Barolli, E. Spaho, F. Xhafa, L. Barolli, M. Takizawa,*Application of GA and Multi-objective Optimization for QoS Routing in Ad-Hoc Networks*,14th International Conference on Network-Based Information Systems (NBiS), Tirana, September 2011.

[9] L. Barolli, A. Koyama, T. Suganuma, N. Shiratori, *A Genetic Algorithm Based QoS Routing Method for Multimedia Communications Over High-Speed Networks*, Information Processing Society of Japan (IPSJ), Vol. 44, No. 3, pp. 544-552, March 2003.

[10] J. Abdulla, D. Parish, *Effect of Mobility on the Performance of GA-based QoS Routing in Mobile Ad Hoc Networks*, International Conference on Intelligent and Advanced Systems, Kuala Lumpur, Malaysia, November 2007.

[11] D. E. Golberg, *Genetic Algorithms in Search, Optimization and Machine Learning*, Book, Addison-Wesley Longman Publishing Co., Inc. Boston, MA, USA 1989.

[12] M. Vavouras, *High-speed FPGA-based implementations of a Genetic Algorithm*, International Symposium on Systems, Architectures, Modelling, and Simulations, Samos, Greece, July 2009.

[13] P. Sateesh Kumar, S. Ramachamndram, *Scalability of Network Size on Genetic Zone Routing Protocol for MANETs*, International Conference on Advanced Computer Theory and Engineering, Phuket, Thailand, December 2008.

 ISBN: 978-1-61208-231-8

A Distributed Protocol for Wireless Sensor Networks Based on Multiple-Leader Stackelberg Network Games

Gautam S. Raj and Volkan Rodoplu
Department of Electrical and Computer Engineering
University of California, Santa Barbara, CA 93106
gautamraj@gmail.com, vrodoplu@ece.ucsb.edu

***Abstract*—While the past literature on game theory rarely addresses the implementation of protocols that converge to Nash equilibria, practical networks must be designed with protocols that correctly address issues of information asymmetries, hysteresis effects due to these asymmetries, and the fact that information can propagate only locally on networks. To this end, we develop a distributed protocol based on multiple-leader Stackelberg network games to efficiently utilize the localized energy resources of a sensor network. Our protocol arrives at a Nash equilibrium of the multiple-leader Stackelberg network game. We demonstrate the performance of our protocol under a large-scale fading model for the internodal links, and quantify its control overhead. Through this work, we find that there are considerable differences between centralized implementations of algorithms that find Nash equilibria on networks, and distributed protocols that can converge to those equilibria in practice.**

***Index Terms*—network, Stackelberg, game, pricing, distributed, protocol**

I. Introduction

Wireless sensor networks are typically conceived of as collective entities that collect information from an area and relay it to a collection site (a.k.a. base station) via a multi-hop network between the sensor nodes. However, decisions in sensor networks have to be made in a localized and distributed manner. Each node usually has a limited battery supply that it has to conserve, and sees different Joules-per-bit costs along the different links to its neighbors, assuming that each node is able to dynamically adjust its transmit power level to reach its neighbors [1]. In addition, sensor networks typically operate in the low traffic load regime; that is, the key measure is not the achieved bits-per-second throughput, but rather the bits-per-Joule capacity [2] of the network, namely the number of bits that can be sent per Joule of energy to the destination. As a result, in sensor networks, most of the bandwidth goes unused, and end-to-end data transmissions typically occur in an on-demand fashion, initiated either by the source that has just collected some important data, or "pulled" from the source by the destination [3].

Game theory models each node as a selfish, autonomous entity that aims to maximize its own utility. Even though the nodes in a sensor network have as their common objective, the reliable end-to-end delivery of sensor data, from the perspective of distributed, localized protocol design, each node can be modeled as an entity that also aims to preserve its battery resources by reflecting the energy costs it is incurring to transfer the information. Then, the most natural setting in which this locally available information is made visible to the network is through pricing variables that are locally determined by the relay nodes.

The application of game theory to routing problems in wireless sensor and ad hoc networks is not new. Sadagopan et al. [4] show the construction of an energy-balanced tree of sensor nodes, modeling each sensor as a selfish entity. Nurmi [5] models energy-constrained routing in ad hoc networks made up of selfish nodes, and lets the source send along the best path based on its subjective beliefs about the amount of remaining energy at the relay nodes. Liu et al. [6] assume that each node forwards with some probability, and take the end-to-end reliability to be the product of these. Under a single-source, single-destination model, they develop a polynomial-time method for deriving a Nash equilibrium routing path. Sengupta et al. [7] apply non-cooperative game theory to power control problems in wireless sensor networks, taking each sensor as a selfish entity. Similarly, Campos-Nanez et al. [8] develop a game-theoretic approach to power management in sensor networks, and Kannan et al. [9] model wireless sensors in a routing game to achieve reliable, energy-constrained routes through the sensor network. Felegyhazi et al. [10] examine cooperative packet forwarding in a game-theoretic framework in multi-domain sensor networks.

None of the above works consider the incorporation of the source's utility function into the decisions of a relay node, as in a Stackelberg framework. In the past, Stackelberg games have been to applied to wired networks with a single Internet Service Provider (ISP) [11]–[13], where the ISP (or a group of multiple ISPs [14]) is the Stackelberg leader, and the network users are the followers. More recently, this model has also been applied to wireless networks [15], again under a single-leader setting. In contrast to these single-leader settings, this paper utilizes the framework of a "multiple-leader Stackelberg game", introduced in [16], in which each relay node acts as a leader that anticipates the response of the source node that is currently initiating traffic to the base station.

 ISBN: 978-1-61208-231-8

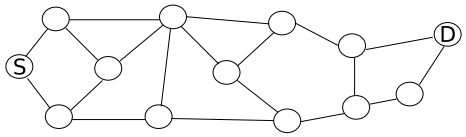


Fig. 1. General network topology.

The main contribution of the current paper is the design of a distributed protocol that converges to a Nash equilibrium of the multiple-leader Stackelberg game. In fact, the Nash equilibrium to which our protocol converges is a Pareto-optimal Nash equilibrium; that is, it is not possible to increase the utility of any one of the users without decreasing the utility of another user. (This fact cannot be proved within the scope of this paper.) Pareto-optimality generalizes scalar capacity to multiple dimensions. Nash equilibria are desirable because they constitute stable operation points from the perspectives of the users in a system. A Nash equilibrium implies that a user cannot benefit from unilateral deviations (i.e., deviations by itself) from the operation point of the network. While this is clearly desirable when users have competing objectives (as in non-cooperative games), it is also desirable in the implementation of *distributed* protocols on sensor networks. In this paper, we model each relay node as an autonomous entity that aims to maximize its own utility. However, the Stackelberg formulation by which each relay node takes into account the utility of the source node creates the link that ties that objectives of the nodes together. Hence, the Stackelberg feature is what makes the protocol useful for application to sensor networks.

While the past literature on the application of game theory to networks rarely addresses the *implementation* of protocols that converge to Nash equilibria, practical networks must be designed with protocols that correctly address issues of information asymmetries between the nodes, hysteresis effects due to these asymmetries, and the fact that information can propagate only locally in these networks. This paper makes an important contribution in this regard in that it explicitly addresses the design of a distributed protocol that overcomes these effects, and further quantifies the overhead of this design in order to show that it is viable. Through this work, we show that there are considerable differences between centralized implementations of algorithms that find Nash equilibria on networks, and those that design distributed solutions.

The rest of this paper is organized as follows: In Section II, we describe our utility and network models. In Section III, we design a distributed network protocol that converges to a Nash equilibrium of the multiple-leader Stackelberg game on this network. In Section IV, we analyze the performance of this protocol when it is applied to energy-limited, ad hoc wireless networks. In Section V, we present our conclusions.

II. Models and Assumptions

In this paper, we consider a sensor network of N nodes on an arbitrary topology G. Since the data generation rates in typical sensor networks (e.g., for habitat monitoring and sensing) can be as low as a few kilobytes per hour, and commercial modems (such as Crossbow [17]) typically operate at relatively high data rates such as 250 Kbits per second, bandwidth usage is not an issue; however, energy consumption is of paramount importance. Due to the low data generation rates, we can focus on the data from a single source to the destination at a time, as shown in Fig. 1. On this topology, the Joules-per-bit cost from each node to any one of its neighbors is fixed, and is independent of the concurrent transmissions on the other links. The constant Joules-per-bit costs (rather than e.g., convex costs) hold if the modulation scheme is fixed (e.g., adaptive modulation is not used). The non-interference assumption is well-justified in the low data rate sensor network scenario (see [18] for a full justification, with numerical examples from sensor network applications.)

Throughout the paper, we focus on a single source at a time. This is possible because the ratio of the total average generated data rate to the available bandwidth is very low in sensor networks. We label the source node as node 1, and the destination node as node N. We let $\aleph$ denote the node set, and $\mathcal{R}$ denote the set of relay nodes; that is, $\mathcal{R} = \{2, \ldots, N-1\}$. In order to reflect back to the source the average energy costs that it bears, each relay node i charges a price p_i per bit, independently of which outgoing link is used for the transmission. Each p_i is a variable under the control of the relay node i. The total price along any path h from the source to the destination is the sum of the prices on h, and this price is assumed to be borne by the source node. These prices merely constitute a distributed scheme to organize and efficiently utilize the network's energy resources.

We focus on the utility of the source node each time that it has accumulated sufficient sensor data to be sent to the destination. However, as mentioned earlier, since the prices reflect the energy costs of transmission to the relay nodes, the source node may end up sending a variable number of bits to the destination, trading off the energy cost of transmission in the relay nodes against the utility gained by sending sensor data to the destination. As in [16], we model the utility of the source node as

$$u_1(b_1) = M_1 b_1^{1/\alpha} - p_{best}^{total}(\mathbf{p}) b_1, \alpha > 1, b_1 \geq 0 \qquad (1)$$

In the above equation, the variable b_1 is the number of bits that the source node chooses to send through the network to the destination node. We call parameter $M_1 > 0$ the "amplitude" of the utility function. The physical meaning of this parameter is that it determines how much value we place on sending sensor data end-to-end. Making this parameter larger means that we place more value on this, relative to the prices that are charged (which reflect the relay nodes' energy costs). The parameter $\alpha > 1$ governs the curvature of the source's utility function. Physically, a small α means that the benefits of sending more bits continue to remain large even as b_1 increases.

The source node always chooses the path with the lowest price to the destination. Above, $p_{best}^{total}(\mathbf{p})$ is the total price of the lowest price path from the source to the destination. It is a function of the vector $\mathbf{p}$, which is the vector of all of the

 ISBN: 978-1-61208-231-8

prices of the relay nodes in the network. Node 1 always acts to maximize its own utility.

The second part of our model focuses on the utility function of each relay node. We assume that a relay node i gains a utility of p_i for each bit that it transmits along one of its outgoing links, and loses a utility equal to the cost of transmitting along that link. Let h_i denote a path of links from the source to the destination, such that the path goes through the node i. Let $c_{i,next}(h_i)$ denote the cost per bit incurred by i to transmit on the link that goes out from i and that falls on the path h_i. Note that this cost may depend on both the Joules-per-bit link cost as well as the remaining battery energy of the relay node. Hence, the notion of cost c_{ij} is general. Then, the utility of relay node i is

$$u_i(p_i) = (p_i - c_{i,next}(h_i))b[h_i] \quad (2)$$

where $b[h_i]$ is the number of bits that the source node chooses to send through node i, along the path h_i. We see that in order to achieve a positive utility, it is necessary that node i set $p_i > c_{i,next}(h_i)$.

Now, one of the key assumptions in our framework is that even though prices are used to arrive at a distributed management of localized resources in a sensor network, overall, the sensor network represents a collective effort to send sensor data end-to-end from the source to the destination. Hence, it is to the network's advantage to incorporate the form of the utility function of the source node into the relay node's decisions. Such schemes are generally referred to as "Stackelberg games" where the leader incorporates into its own utility function, the form of the utility function of the follower. Here, the source node is the follower, and each of the relay nodes acts as a leader, hence, resulting in the novel form of a multiple-leader Stackelberg game. Based on this discussion, the utility model of a relay node i is given by

$$u_i(p_i; p_{-i}) = (p_i - c_{i,next}(h_i))b_1[h_i](p_i; p_{-i}) \quad (3)$$

where p_{-i} denotes the set of prices of all of the relay nodes besides i, and $b_1[h_i](p_i; p_{-i})$ is the number of bits that Node 1 sends through node i via path h_i, after it has chosen the lowest price path and the number of bits to send through that path, via its maximization of its own utility in (1). (Note that if node i is not on the lowest price path, then $b_1[h_i](p_i; p_{-i}) = 0$; that is, no bits are sent through node i.)

III. Distributed Protocol Design

In [16], we described a centralized algorithm to find a Nash equilibrium of the network over an arbitrary topology G of relay nodes. In this paper, we describe a distributed network protocol that the nodes can use in practice to converge to a Nash equilibrium. The distributed protocol that we present converges to a Nash equilibrium because it implements the centralized algorithm of [16] whose convergence to a Nash equilibrium was proved. The main idea behind the convergence of this protocol is as follows: we designed an algorithm on a general topology that converged to a Nash equilibrium by solving a set of price equations via the Jacobi method. The same Jacobi method is implemented via the distributed protocol, as will be seen shortly for the serial network. After this, the competition that occurs between parallel paths within the network is modeled by the protocol's dynamically placing caps on the prices on the currently winning path via the constraints that occur due to the competition paths. The main challenge that we have to address in this setting is that each node can communicate only with its neighbors on the topology G; hence, no global information channels that can announce all of the prices of the relay nodes to each other exist. Further, the source node can become aware of the relay node prices only through its own links on G, and any announcements by the source node, of the best current bid (that is, the best current lowest price path) must propagate to all of the relay nodes via the links on G.

Finally, the control overhead of the resulting network protocol must be small enough to justify its use in sensor networks. We shall demonstrate this in the next section.

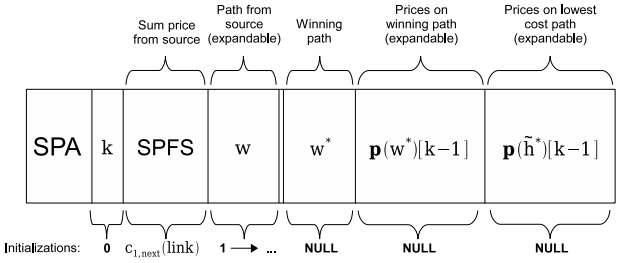


Fig. 2. SPA Packet

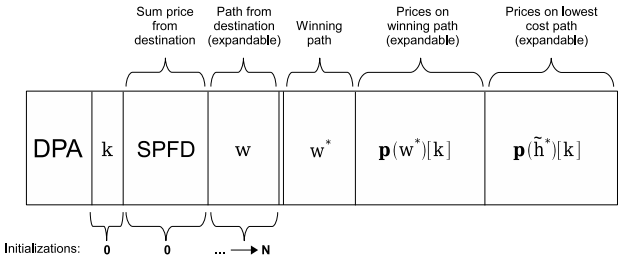


Fig. 3. DPA Packet

A. Distributed Protocol on a Serial Network

For ease of exposition, we begin by developing the protocol first for the serial network of Fig. 4. In a serial network, every relay node needs to update its price p_i according to (see (11) in [16]):

$$\forall i \in \mathcal{R} : p_i^* = (\alpha - 1)\Big[\sum_{j \in \mathcal{R}\setminus\{i\}} p_j^* + c_{12}\Big] + \alpha c_{i,i+1} \quad (4)$$

The sum of the prices of all of the other relay nodes can be efficiently accumulated as follows: The source node initiates a "Source Price Accumulate" (SPA) packet, and sends it on its link to Node 2 in Fig. 4. The ultimate destination of this packet is Node N. The structure of this packet is shown in Fig. 2. The second field is the iteration number k of the protocol, which is set to 0 for the first SPA that the source ever sends out. The third field of this packet is the "Sum Price From

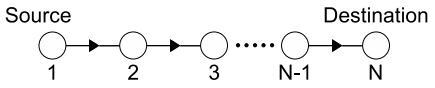


Fig. 4. An N-node serial network.

Source" (SPFS), which accumulates the total sum price from the source node thus far. Node 1 initializes this field to c_{12}, which is the cost of the link from 1 to the next node on which this SPA is being sent. (This is denoted by $c_{1,next}(w)$ in the figure, where w is the path that this SPA travels on.) We shall now describe the events for the kth iteration. When Node 2 receives the SPA, it records the price accumulated from the source thus far, and adds its own current price $p_2[k]$ to this field. In the 0th iteration, $p_2[0] = c_{23}$, which is the cost of the link to the next node. The fourth field w is an expandable list, that contains the path through which the SPA has travelled thus far. Hence, Node 2 also adds its node ID to the path w in the fourth field, and sends the SPA to Node 3. Node 3, and all of the relay nodes in this sequence continue in a similar fashion.

When the SPA packet has reached the destination node N, all of the relay nodes have accumulated the sum of the prices of the relay nodes to their left on the serial network, via the SPFS field. When Node N receives the SPA, it records the path w which contains all of the nodes through which the SPA travelled, as well as the total price, namely the value of the SPFS field, accumulated through the entire path. Then, Node N initiates a "Destination Price Accumulate" (DPA) packet toward the source node. The structure of the DPA packet is shown in Fig. 3. The third field in the DPA is the "Sum Price From Destination" (SPFD), which accumulates the sum of the prices on the *forward* links toward the destination. Because there is only one path from the source to the destination in a serial network, Node N sets w^*, the "winning path" field of the DPA, to the path w of the SPA that it has just received. Note that the sixth field of the DPA, $\mathbf{p}(w^*)$ is an expandable vector of prices. This field is initially empty, and will be updated by the relay nodes on the winning path w^*, as the DPA travels back.

When a relay node i receives the DPA, it records the value of the SPFD field. At this point, the relay node i has the sum of the prices of all of the other relay nodes, obtained from the SPFS field of the SPA, and the SPFD field of the DPA. Thus, it now updates its price $p_i[k+1]$ according to (4). Then, it adds its current price, $p_i[k+1]$ to the SPFD field, and sends it toward the source node. Hence, when the DPA has reached the source node, all of the relay nodes have updated their prices. Further, the source has just received the winning path w^* from the fifth field of the DPA, as well as all of the *new* prices on the winning path, namely $\mathbf{p}(w^*)$ from the fifth and sixth fields of the DPA.

After the source has received the DPA of the kth iteration, it first checks whether the prices on the winning path w^* have converged. It does this by taking the norm of the difference between the prices on w^* in the current and the previous iterations. If the prices on w^* have converged, then

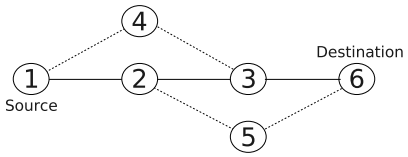


Fig. 5. Example topology.

it terminates the SPA-DPA exchanges, and announces the final path w^{**} via a separate packet to all of the nodes. Otherwise, it prepares a new SPA packet, with iteration number $k+1$ in the second field, and with the currently winning path w^* that it has copied from the DPA into the fifth field of the SPA, and sends this SPA toward the destination.

B. Distributed Protocol on the General Topology

The distributed protocol on the general topology will implement a distributed version of the centralized algorithm in Fig. 3 of [16]. The centralized algorithm has access to all of the constraint equations on the least cost path $\tilde{h}^*$. In contrast, in the distributed protocol, the nodes do not know the $\tilde{h}^*$ path a priori, and have no global picture of the constraints on the $\tilde{h}^*$ path. Hence, both $\tilde{h}^*$ and the price constraints have to be discovered dynamically, while the price competition takes place among the relay nodes. A part of the main structure of the protocol is the SPA-DPA exchanges described for the serial network in the previous subsection. The pseudocode for the distributed protocol is shown in Figs. 6-9. On a general topology, on line 12 of Fig. 6, the source initiates an SPA along each of the paths that emanate from it. On lines 16-26 of Fig. 7, when a relay node i receives an SPA, it first checks the accumulated price thus far (namely the value of the SPFS field) against *minSPFS* which is an internal variable of i, set to the minimum SPFS value observed so far. If the value of the SPFS field is greater than the value of *minSPFS*, then it discards the SPFS field of this SPA. Otherwise, a better total price from the source up to this relay node has been discovered; hence, *minSPFS* is updated to the value of the SPFS of this SPA.

We shall now describe the protocol for the example network in Fig. 5. We define an iteration as one SPA-DPA exchange from the source back to the source. In iteration 0, the source starts the competition round by sending an SPA to Nodes 2 and 4. Nodes 2 and 4 record the current path w, and the SPFS from the SPA. After storing these fields, they append their node IDs to the w field, and add their link costs to the SPFS fields of their respective SPAs. In this example, Node 4 will add its current price (which is c_{43} in this iteration), while Node 2 will add its current price (c_{23} in this iteration) when sending to node 3, and c_{25} when sending to Node 5. Then, they forward the SPAs to their next nodes, who repeat the process, until all of the SPAs reach the destination. The set of "next nodes" of any node i is defined as the set of all of its neighbor nodes except the ones in the w field of the SPA. (This prevents loops.) These actions are shown on lines 16-26 of Fig. 7.

For the destination node, the *Receive* function on line 8 of

 ISBN: 978-1-61208-231-8

```
1  // Internal Variables
2  int K_MAX=_K_MAX; // max iterations
3  int J_MAX=_J_MAX; // max nodes
4  minSPFD[K_MAX] = [LARGE,...,LARGE]; //min sum price from dest.
5  minW = NULL; //min price route from destination
6  k = 0; //sequence number of SPA
7  p[J_MAX][K_MAX];
8  δ = DELTA;
9  p[∗][−1] = LARGE;
10 links = this→allOutgoingLinks;
11 // Main Function
12 send_SPA(links,k,c1,next(links),1,NULL,NULL,NULL);
13 k++;
14 while (TRUE) {
15   while (Receive(DPA[k])) { //Receive all DPA's for kth iteration
16     [spfd, w; w*, p[w*][k], p[h̃*][k]] = ExtractFields(DPA[k]);
17     if (spfd < minSPFD[k]) {
18       minSPFD[k]=spfd;
19       minW = w;
20     }
21   } // Got all DPAs for iteration k
22   w* = w;
23   if (k == 0)
24     h̃* = w;
25   else if (||p[w*][k] − p[w*][k − 1]|| < δ | k == K_MAX) {
26     send(w**, links); //announce final path
27     break;
28   }
29   send_SPA(links,k, c1,next(links), 1, w*, p[w*][k], p[h̃*][k]);
30   k++;
31 }
```

Fig. 6. Distributed protocol executed by the source node.

Fig. 9 has a built-in timer that stops listening for new SPA packets after a timeout has been reached. The timeout must be as long as needed to receive the SPA packets on all of the closest competition paths, and depends on the network size N. If all of the nodes were in a linear arrangement, then the timeout must grow linearly with N. If the nodes are randomly deployed on a square region, then, since the average number of hops from a source at one end to a destination at another grows as $\mathcal{O}(\sqrt{N})$, the timeout must grow in this fashion with respect to N, with the coefficient of the growth larger for a smaller probability that the SPA's from not all of the paths may have arrived by that time. (A design that aims at no loss from optimality uses a design that grows linearly with N in all cases.)

In iteration 0, once the destination receives all the SPAs, it computes the lowest-cost path $\tilde{h}^*$, by finding the minimum SPFS, and using the corresponding w. Then, the destination creates a DPA and sends it toward the source, on nodes 3 and 5 in Fig. 5, as shown on line 15 of Fig. 9. In iteration 0, each relay node that receives the DPA records the lowest-cost path $\tilde{h}^*$, from the w^* field of the DPA, as shown on lines 29-31 of Fig. 7. Each relay node also adds its node ID to the w field, and its current price (which is its link cost in iteration 0) to the SPFD field (lines 59-66). At this point, the node can compute its price for the next iteration, using (4). If the node sees from the DPA that it is on w^* for the 0th iteration, it also appends its price to the $\mathbf{p}(w^*)[0]$ and $\mathbf{p}(\tilde{h}^*)[0]$ fields of the DPA (line 60). This is done at each node for each DPA packet that it receives. Once the source receives all the DPAs, it must determine the winning path w^* for iteration 0. To do this, as shown on lines 15-22 of Fig. 6, it finds the minimum SPFD value from all the DPAs, and records the corresponding path

```
1  // Internal Variables
2  int K_MAX=_K_MAX; // max iterations
3  int J_MAX=_J_MAX; // max nodes
4  minSPFS[K_MAX] = [LARGE,...,LARGE] // min sum price from source
5  minW_FS[K_MAX] = [NULL,...,NULL] // min price path from source
6  minSPFD[K_MAX] = [LARGE,...,LARGE] // min sum price from dest
7  minW_FD[K_MAX] = [NULL,...,NULL] // min price path from dest
8  w*[K_MAX]; // winning path for iteration k
9  h̃* = w*[0]; // lowest cost path
10 priceLocked = FALSE;
11 nodesConstrained = ∅;
12 //Main Function
13 i = this→nodeID;
14 links = this→allOutgoingLinks;
15 while (TRUE) {
16   while (Receive(SPA[k])) {
17     [spfs,w_SPA,w*[k], p[w*][k], p[h̃*][k]] = ExtractFields(SPA[k]);
18     if (i ∉ w_SPA) { // Prevent loops
19       if (spfs < minSPFS[k])
20         minSPFS[k] = spfs;
21       foreach (link ∈ links)
22         if (link→nodeID == nextNode(h̃*))
23           send_SPA_Link(link,k,spfs + p[i][k], w_SPA+→ i);
24         else
25           send_SPA_Link(link,k,spfs + ci,next(link),w_SPA+→ i);
26     }
27   }
28   while (Receive(DPA[k])) {
29     [spfd, w_DPA, w*] = ExtractFields(DPA[k]);
30     if (i ∉ w_DPA && spfd < minSPFD[k])
31       minSPFD[k] = spfd;
32     if ((i ∉ h̃*) || (nextNode(w_DPA) != nextNode(h̃*)))
33       p[i][k] = ci,next(w_DPA); // Return link cost
34     else if (i ∈ w*[k] && nextNode(w_DPA) ∈ w*[k]) { // On w*[k]
35       k_last = k; // Store last time on best path
36       if (priceLocked)
37         p[i][k + 1] = p[i][k];
38       else if ((nodesConstrained\w*[k]) ! = ∅) {
39         p[i][k + 1] = p[i][k];
40         willLock = FALSE;
41       }
42       else if (nodesConstrained ⊆ w*[k] && willLock) {
43         priceLocked = TRUE;
44         p[i][k + 1] = p[i][k];
45         nodesConstrained = ∅;
46       }
47       else if (h̃* ∩ w*[k] ≠ ∅)
48         p[i][k + 1] = p[i][k];
49       else { // Node is not locked, so unfreeze price updates
50         SumOtherPricesOnPath[k] = minSPFS[k] + minSPFD[k];
51         p[i][k + 1] = (α − 1)SumOtherPricesOnPath[k]+αci,next(h̃*);
52       }
53     }
54     else { // Not on w*[k]
55       [ϵ, nodesConstrained] =
           Surplus(w*[k_last], w*[k], p[][k_last], p[][k], i);
56       p[i][k + 1] = p[i][k] + ϵ  Σ_{j∈nodesConstrained} (p[j][k] − p[j][k_last])
57       willLock=TRUE;
58     } // Finished computing price, now send DPA
59     if (i ∈ w* && i ∈ h̃*)
60       send_DPA(links,k,spfd+p[i][k],(w_DPA)+→ i, p[i][k], p[i][k]);
61     else if (i ∉ w* && i ∈ h̃*)
62       send_DPA(links,k,spfd+p[i][k+1],(w_DPA)+→ i,NULL, p[i][k+1]);
63     else if (i ∈ w* && i ∉ h̃*)
64       send_DPA(links,k,spfd+p[i][k],(w_DPA)+→ i, p[i][k],NULL);
65     else
66       send_DPA(links,k,spfd+p[i][k],(w_DPA)+→ i,NULL,NULL);
67   }
68   if (Receive(w**)) {
69     if (i ∈ w**) lockedPrice = p[i][k];
70     break;
71   }
72 }
```

Fig. 7. Distributed protocol executed by each relay node.

w as w^*.

In iteration 1, the source initiates the SPA using the w^* and the node prices from iteration 0. Once a relay node i receives an SPA, it appends its price $p_i[0]$ to the SPFS field

1 [ϵ,nodesConstrained]=Surplus($w^*(k-1), w^*(k), p[][l], p[][k], i$) {
2 [oldPath,newPath] = FindRemovedSegment($w^*(l), w^*(k), i$);
3 cap = $\sum_{j \in \text{newPath}} p[j][k]$;
$$\epsilon = \frac{\text{cap} - \sum_{j \in \text{oldPath}} p[j][l]}{\sum_{j \in \text{oldPath}} (p[j][k] - p[j][l])};$$
5 }

Fig. 8. Surplus subroutine for the relay nodes.

```
1   // Internal Variables:
2   K_MAX = _K_MAX;
3   minSPFS[K_MAX] = [LARGE,...,LARGE];
4   k = 0;
5   // Main function
6   links=this→allOutgoingLinks;
7   while (TRUE) {
8     while (Receive(SPA[k])) {
9       minSPFS = LARGE;
10      [spfs, w, p(h̃*)] = Extract(SPA[k]); // Uses Sequence No. of SPA
11      if (spfs < minSPFS[k]) {
12        minSPFS[k] = spfs;
13        w* = w;
14      } // Got all SPAs for iteration k
15        send_DPA(links,k,0,this→nodeID,w*,NULL,NULL);
16      k++;
17      }
18    }
```

Fig. 9. Distributed protocol executed by the destination node.

and its node ID to the w field, and forwards the SPA to its next nodes (lines 16-26, Fig. 7). The destination node now computes w^* for iteration 1, by finding the minimum SPFS value, and sends out DPAs on all of its outgoing links (lines 8-17, Fig. 9). When a relay node receives a DPA packet for iteration 1, it checks if it is on w^*, and if so, it appends its price for the current iteration to $\mathbf{p}(w^*)[k]$ and $\mathbf{p}(\tilde{h}^*)[k]$. Then, it computes its price for the next iteration, and forwards the DPA to its next nodes (lines 59-66, Fig. 7).

Returning to our example in Fig. 5, suppose that in iteration k, Node 2 receives a DPA in which Node 2 is *not* on w^*. In this case, because Node 2 is on $\tilde{h}^*$, it will append its price for iteration k to the SPFD and $\mathbf{p}(\tilde{h}^*)[k]$ fields, and forward it to all of its next nodes. Node 2 would like to lower its price to return to w^*, but it does not know the constraint cap imposed on it; that is, it does not know $c_{14} + c_{43}$. Hence, it must wait for the SPA in iteration $k+1$ to travel on the path $1 \to 4 \to 3 \to 6$, and then for a DPA in iteration $k+1$ to inform Node 2 of the prices of the nodes in the constraint, which is only Node 4 in this case. Once Node 2 receives the DPA for iteration $k+1$, it computes the cap from $\mathbf{p}(w^*)[k]$, and interpolates its price back using the Surplus subroutine of Fig. 8. Then, it immediately adds this new price to the SPFD and $\mathbf{p}(\tilde{h}^*)[k]$ fields of the DPA, and forwards it to all of its next nodes. This is done to ensure that Node 2 can return to w^* as quickly as possible. Since this is the only constraint imposed on it in Fig. 5, Node 2 will return to w^* in iteration $k+2$. Because the constraint cap is satisfied with equality, Node 2 can now lock its price for the remainder of the iterations (lines 54-58, Fig. 7).

In general, we may have multiple relay nodes that together exceed some constraint cap. In this case, we would like all the nodes that are capped by the same constraint to act together to reduce their prices, such that the sum of their prices is exactly equal to the cap. Any contiguous segment of nodes that is removed from $\tilde{h}^*$ has encountered some constraint imposed on it. We denote this segment of nodes on $\tilde{h}^*$ by $\mathcal{R}_1$, and the constraining set of nodes by $\mathcal{C}_1$. In the Surplus subroutine of Fig. 8, *FindRemovedSegment* on line 2 returns the contiguous set of removed nodes $\mathcal{R}_1$, of which relay node i is a member. On line 3, node i sums the prices of the nodes in $\mathcal{C}_1$ to determine the constraint cap that is imposed on it, and on line 4, it computes the surplus.

When multiple nodes exceed this constraint cap, increasing any of the nodes' prices would violate the cap; hence, we freeze the price updates for all the nodes on $\mathcal{R}_1$ (lines 42-46, Fig. 7). However, after this, if only a subset of the nodes in $\mathcal{R}_1$ has returned to w^*, this implies that there is another constraint acting on them (lines 38-41, Fig. 7). We denote this smaller subset by $\mathcal{R}_2$, and the new set of constraining nodes by $\mathcal{C}_2$. At this point, we temporarily freeze the prices of all the nodes that have returned to w^*, namely $\mathcal{R}_1 \setminus \mathcal{R}_2$. Then, the nodes in $\mathcal{R}_2$ interpolate their prices again (lines 54-58, Fig. 7), using the new segment of contiguous nodes and the new cap, imposed by $\mathcal{C}_2$. Let m be the number of nodes on segment $\mathcal{R}_1$. Then, after $\mathcal{O}(m^2)$ applications of this procedure, all of the relevant constraints for $\mathcal{R}_1$ will have been discovered, and hence, all the nodes on $\tilde{h}^*$ will have returned to w^*.

Although all the nodes on $\mathcal{R}_1$ have returned to w^*, their prices are not in Nash equilibrium: Even though we initially set the sum of the prices for the nodes on $\mathcal{R}_1$ equal to the cap $\mathcal{C}_1$ with equality, at the end of the above procedure, this is no longer the case. In fact, only the last set of nodes in the procedure to return to w^* are set exactly equal to the final cap. In Fig. 7, the variable *willLock* is TRUE only for this set of nodes. Hence, we permanently lock the prices of the last nodes to return to w^*, and allow all the other nodes in $\mathcal{R}_1$ to resume monopoly pricing (lines 42-46, Fig. 7). This process continues for the rest of the nodes until the prices of the nodes have converged, or until K_{MAX} has been reached (lines 25-28, Fig. 6).

IV. Simulation Results

We simulate the distributed protocol of Section III, using the same random node placement and link costs as of the centralized protocol simulations, as in [16]. The dominant factor in the convergence to Nash equilibrium is the number and structure of the competing paths; however, it is difficult to characterize analytically the dependence of the convergence rate upon such a complex factor. As a remedy, we examine the convergence rate of the protocol via the simulation studies in this section. It should be noted that the simulation studies in this section should be read as a sequel to the simulation studies in [16]. We also compute the control overhead of our protocol and show that it is reasonable for use in sensor networks. Figs. 10(a) and 10(d) show ensemble average results taken over 200 simulations with $N = 50$ nodes, and $\alpha = 1.5$, while Figs. 10(b) and 10(c) display particular realizations. For Figs. 10(a) and 10(d), an average over 200 simulations is sufficient since both the oscillations of the price in Fig. 10(a),

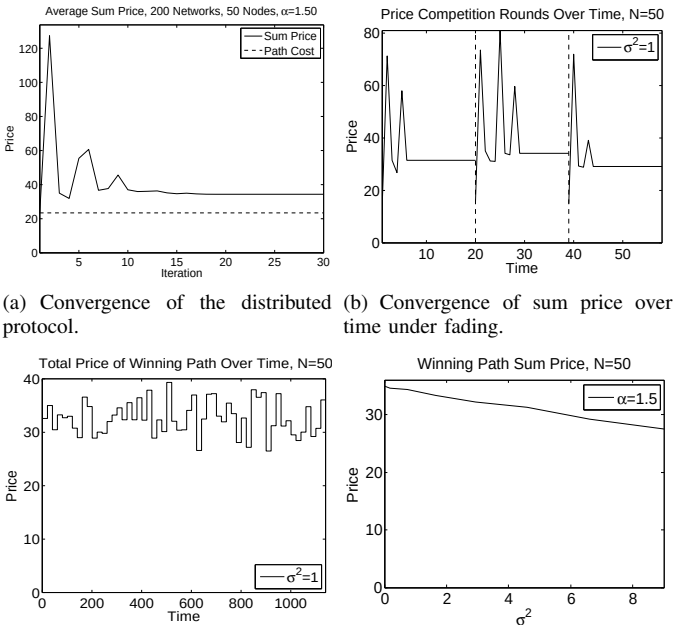
 ISBN: 978-1-61208-231-8

and the monotonic decrease of the price of the winning path in Fig. 10(d) display their clear trends.

Fig. 10(a) shows the price of the currently winning path w^* as a function of the number of iterations, when the distributed protocol of Section III is used. We see three successive peaks, which correspond to price-adjusting cycles. The first peak corresponds to the price increase in the first iteration. Because the price of all the nodes are initially free to change, this peak corresponds to every node's incrementing its price, and consequently is the largest. Each successive peak is lower, because as more nodes lock their prices, there are fewer nodes raising their prices. In addition, some of the networks we average converge within 1 or 2 price-adjusting cycles, thereby reducing the average height of the latter peaks. It takes 18 iterations for the average price to converge. The difference between the final sum price and the initial path cost is the ensemble average of the sum of the surplus of all relay nodes.

We calculate the control overhead of our protocol as follows: Let n_p denote the number of price iterations until convergence. Per iteration, each relay transfers 1 SPA and 1 DPA packet. Let N denote the number of nodes in the network. Then, $\lceil \log_2(N) \rceil$ bits are needed to encode the node IDs. The maximum possible number of hops in the network is $N-1$. Let b_p denote the number of bits of quantization for the price, in fixed-point representation. Then, in the fields of an SPA (or DPA) packet, it takes $\lceil \log_2(n_p) \rceil$ bits to encode the number of iterations so far, $\lceil \log_2(N) \rceil$ bits times $\lceil N-1 \rceil$ hops to encode the path of node IDs, the same number of bits to encode the winning path, b_p bits times $N-1$ hops to encode the prices on the winning path, and b_p bits times $N-1$ to encode the prices on the lowest cost path. This worst-case control overhead analysis thus shows that a total of $\lceil \log_2(n_p) \rceil + 2(N-1)\lceil \log_2(N) \rceil + 2b_pN$ bits per SPA (or DPA) packet. Hence, per iteration, each relay node transfers a control overhead of twice this amount (1 SPA and 1 DPA), that is, a total of $2(\lceil \log_2(n_p) \rceil + 2(N-1)\lceil \log_2(N) \rceil + 2b_pN)$ bits of control overhead until convergence to the equilibrium prices. Hence, the control overhead grows as $\mathcal{O}(\mathcal{N} \log_{\in}(\mathcal{N}))$ for large-scale sensor network deployments. However, assuming midsize deployments, the exact numbers might be more important than asymptotic growth. For example, for a network of 100 sensor nodes, and with $b_p = 8$ bits, and $n_p = 10$ iterations, the control overhead is 5980 bits. Let f be the fraction of the tolerable control overhead compared with sensor network data. Then, if $f = 0.01$, then 598 kbits of sensor data need to be accumulated for the control overhead to be justified.

Fig. 10(b) shows the effects of large-scale fading on successive price competition rounds when the distributed protocol is used. We have used a log-normal distribution to model fading on the links between the relay nodes. (Since the sensor nodes are stationary in many settings, the source of the lognormal shadowing variations that we model are due to the variations of the obstacles in between, e.g., in an urban setting. When sensor nodes are placed over such a terrain, the channel between the nodes is rarely static, but rather show significant variations due to the variations in the urban clutter



(a) Convergence of the distributed protocol.

(b) Convergence of sum price over time under fading.

(c) Equilibrium prices over time under fading.

(d) Trend in total winning-path price with fading parameter σ.

Fig. 10. Simulation results for the distributed protocol.

in between.) Specifically, the link costs are recomputed each round as $c_{ij} = d_{ij}^4 \times 10^{(L_{ij}/10)}$, where $L_{ij} \sim \mathcal{N}(0, \sigma^2)$, and are independent for each link ij, and at each round. It is assumed that the coherence time is longer than the convergence time; that is, the link costs are fixed within each competition round. We see that for the same network, varying link costs can have an impact on both the equilibrium price, and the rate of convergence. In the second competition round, three price-adjusting cycles are needed to reach a Nash equilibrium, whereas only two are needed in the first and third. (Note that in our control overhead calculation, we allowed for up to 10 iterations, and the simulations show that this maximum still holds under fading. Hence, the control overhead calculation is still valid.) Fig. 10(c) shows the variation of equilibrium prices under fading.

In Fig. 10(d), we see that large-scale fading reduces the total price of the winning path. As the variance of the L_{ij} increases, the winning-path sum price decreases. Because large-scale fading reduces the costs of some of the links in the network, the protocol is able to take advantage of this and find new lower-cost paths as σ increases.

V. Conclusion and Future Work

We have presented a distributed protocol for wireless sensor networks, based on multiple-leader Stackelberg games. These games allow the relay nodes, each of which acts as a Stackelberg leader, to incorporate the utility function of the source into their utilities. We have designed a distributed protocol to arrive at a Nash equilibrium of the game. We have also shown the convergence of the protocol to the Nash equilibrium as a function of time, and quantified its control overhead. In our future work, we aim to generalize this model to a network

 ISBN: 978-1-61208-231-8

with multiple source and multiple destinations.

REFERENCES

[1] V. Rodoplu and T. Meng, "Minimum energy mobile wireless networks," *IEEE J. Select. Areas Commun.*, vol. 17, no. 8, pp. 1333 – 1344, Aug. 1999.

[2] ——, "Bits-per-joule capacity of energy-limited wireless networks," *IEEE Transactions on Wireless Communications*, vol. 6, no. 3, pp. 857–865, 2007.

[3] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed diffusion for wireless sensor networking," *IEEE/ACM Trans. Netw.*, vol. 11, no. 1, pp. 2–16, 2003.

[4] N. Sadagopan, M. Singh, and B. Krishnamachari, "Decentralized utility-based sensor network design," *Mobile Networks and Applications*, vol. 11, pp. 341–350, 2006.

[5] P. Nurmi, "Modeling energy constrained routing in selfish ad hoc networks," in *Proceeding from the 2006 workshop on Game theory for communications and networks*, ser. GameNets '06. ACM, 2006.

[6] H. Liu and B. Krishnamachari, "A price-based reliable routing game in wireless networks," in *GameNets '06: Proceeding from the 2006 workshop on Game theory for communications and networks*. ACM, 2006, p. 7.

[7] S. Sengupta, M. Chatterjee, and K. Kwiat, "A Game theoretic framework for power control in wireless sensor networks," *IEEE Transactions on Computers*, vol. 59, no. 2, pp. 231–242, 2010.

[8] E. Campos-Nanez, A. Garcia, and C. Li, "A Game-theoretic approach to efficient power management in sensor networks," *Operations Research-Baltimore*, vol. 56, no. 3, pp. 552–561, 2008.

[9] R. Kannan and S. Iyengar, "Game-theoretic models for reliable path-Length and energy-constrained routing with data aggregation in wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 6, pp. 1141–1150, 2004.

[10] M. Felegyhazi, J. Hubaux, and L. Buttyan, "Cooperative packet forwarding in multi-domain sensor networks," in *Third IEEE International Conference on Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops*, 2005, pp. 345–349.

[11] Y. Korilis, A. Lazar, and A. Orda, "Achieving network optima using Stackelberg routing strategies," *IEEE/ACM Transactions on Networking (TON)*, vol. 5, no. 1, pp. 161–173, 1997.

[12] T. Başar and R. Srikant, "A Stackelberg network game with a large number of followers," *Journal of Optimization Theory and Applications*, vol. 115, no. 3, pp. 479–490, 2002.

[13] H. Shen and T. Başar, "Differentiated Internet pricing using a hierarchical network game model," *Proceedings of the 2004 American Control Conference*, vol. 3, pp. 2322–2327 vol.3, July 2004.

[14] S. Shakkottai and R. Srikant, "Economics of network pricing with multiple ISPs," *IEEE/ACM Trans. Netw.*, vol. 14, no. 6, pp. 1233–1245, 2006.

[15] M. Bloem, T. Alpcan, and T. Başar, "A Stackelberg game for power control and channel allocation in cognitive radio networks," in *Proc. IEEE ICST*, 2007, pp. 1–9.

[16] V. Rodoplu and G. Raj, "Computation of a nash equilibrium of multiple-leader stackelberg network games," in *2010 Fifth International Conference on Systems and Networks Communications*, ICSNC 2010, pp. 232–237.

[17] "MICAz OEM edition data sheet," Crossbow, San Jose, CA, USA.

[18] V. Rodoplu and T. Meng, "Core capacity region of energy-limited, delay-tolerant wireless networks," *IEEE Transactions on Wireless Communications*, vol. 6, no. 5, pp. 1844–1853, 2007.

 ISBN: 978-1-61208-231-8

When Wireless Sensor Networks Meet Robots

Giuseppe Amato*, Mathias Broxvall§, Stefano Chessa‡, Mauro Dragone†, Claudio Gennaro*,
Claudio Vairo*
*ISTI-CNR
†University College of Dublin
‡Università di Pisa
§Örebro Universitet
Email:Giuseppe.Amato@isti.cnr.it,mb1@aass.oru.se,ste@di.unipi.it,Mauro.Dragone@ucd.ie,
claudio.gennaro@isti.cnr.it, claudio.vairo@isti.cnr.it

***Abstract*—Enabling integrated robots and Wireless Sensor Network (WSN) applications is an important and extended challenge for both robotics and WSN research & development and a key enabler for a range of advanced hybrid applications, such as environmental monitoring and Ambient Assisted Living (AAL). This paper describes a work-in-progress WSN/robots communication framework that is being purposefully built to facilitate the constructions of robotic ecologies, i.e. networks of heterogeneous computational nodes interfaced with sensors, effectors and mobile robot devices. This paper discusses a number of requirements characterizing this type of systems and illustrates how they are being addressed in the design of the new communication framework.**

***Keywords*-Robots; Wireless Sensor Networks.**

I. INTRODUCTION

A WSN is a wireless network composed by a number of sensors, each of which is an autonomous microsystem capable of sensing a number of environmental parameters (depending on the nature and number of transducers it embeds) and of locally processing and storing sensed data. While WSNs are perfect in monitoring the environment and detecting what is happening in it, they are very limited in reacting to what they detect. Robots, on the other hand, can act as interfaces to WSN solutions and also enhance them by providing important benefits such as sensor deployment, calibration, failure detection and power management.

On the other hand, developing integrated robots & WSN applications has the potential to solve many problems that hinder the spread of pure robotics solutions; in particular, the difficulty of understanding their environment with noisy and imprecise sensor capabilities. In contrast, integrated robot & WSN solutions advocate the augmentation of the robots' communication and interaction capabilities with those afforded by the sensors and services embedded within the environment.

The work described in this paper, which is a work in progress, is being conducted within the context of the EU FP7 project RUBICON, (Robotic UBIquitous COgnitive Network). The project will develop a self-sustaining, adaptive robotic ecology consisting of mobile robotic devices, sensors, effectors and appliances cooperating to perform complex tasks such as supporting an older person to live independently. These components will encourage and teach one another in order to achieve their goals more efficiently and to adapt to changing requirements and user's needs. This will reduce the need for pre-programming and human supervision, and so will make these systems much cheaper and simpler to deploy in a variety of applications, for different homes and users.

One of goals of the RUBICON project is the integration of robot and WSN technologies in order to test them in a real AAL environment. The system will use the network of wireless sensors and actuators, supplemented by a mobile robot, to learn to better recognize situations and activities in the AAL scenario.

Practical implementation of RUBICON's outcomes could be used for:

- Assisting the user in their daily living (e.g. closing the blinds when the user is sleeping).
- Gathering data for post process analysis.
- Monitoring of people at risk.
- Collecting information that will assist in clinical assessments.
- Identifying and alerting relevant stakeholders of potentially dangerous behavior and/or situations.

While the emphasis of our extended research is to provide learning solutions for this type of systems, in order to support our vision we need flexible communication capabilities able to connect components across different nodes and allow sharing of data and learning information, while changing communication path-ways in response to changing circumstances, due to mobility, network disruptions, failures, etc.

Supporting varying computational constraints is a primary priority, as target environments will contain devices such as computers with large processing and bandwidth capacities, as well as much simpler devices such as micro-controller-based actuators and sensor nodes, and even devices with no (customizable) computational capability at all, such as Radio Frequency Identifications (RFIDs).

 ISBN: 978-1-61208-231-8

While existing robot/WSN combined approaches investigate many related issues such as cooperative monitoring, localization and navigation, they often rely on ad-hoc communication mechanisms that usually lack a broader applicability and that do not fully embrace the robotic ecology concept. For instance, most of the existing solutions adopt a centralized integration approach, or apply a data-centric perspective, in which WSNs are treated as just another input to traditional control architectures.

In contrast, we are building a communication framework on top of state of the art robotic and WSN middleware that is purposefully designed to address the characteristic requirements dictated by robotic ecology solutions.

Noticeably, our communication framework is general and it allows the building of several different applications all involving the integration of the moving and actuation capabilities of autonomous mobile robots and the sensing and interacting capabilities of WSN nodes.

The remainder of the paper is organized in the following manner: Section II provides an overview of the most significant robot/WSN integration approaches attempted in past research, focusing on how they have addressed the communication requirements. Section III discusses the requirements and the high-level design of our new communication framework. Section IV details the layered architecture of the framework. Finally, Section V summarizes the contributions of this paper and discusses our plans for future work.

II. Related Work

There are many example of related work combining mobile robots with wireless sensor networks. The latter are usually used to report events that need further investigation and intervention by the robots in the environment whereas robots' mobility helps the WSN to monitor and operate in a larger area than is possible with fixed sensor deployments. For instance, a Mobile Robot is used in [1] to collect sensed data from a WSN in order to prolong the lifetime of the sensor nodes, and also to reduce the hop count cost, when the WSN is partitioned in islands.

Mohammad Rahimi et al. [2] studied the feasibility of extending the lifetime of a wireless sensor network by exploiting mobile robots that move in search of energy, recharge, and deliver energy to immobile, energy-depleted nodes.

With the PlantCare project, [3] have demonstrated how a robot can be used to deploy and calibrate sensors, detect and react to sensor failure, deliver power to sensors, and otherwise maintain the overall health of the wireless sensor network. Navigation strategies employing WSNs usually rely on the fact that the positions of all network nodes are well known or can be inferred. The solutions for the localization problem often employ RSSI readings, which are well documented as unreliable in dynamic environments, to determine node or robot positions [4] , often as part of Robot SLAM (Simultaneous Localization and Mapping) solutions [5].

Batalin [6] addresses the problem of monitoring spatiotemporal phenomena at high fidelity in an unknown, unstructured, dynamic environment. The robot explores the environment, and based on certain local criteria, drops a node into the environment, from time to time. Sensor nodes act as signposts for the robot to follow, thus obviating the need for a map or localization on the part of the robot.

All these solutions for the integration of WSN and mobile robotics usually are developed to solve specific problems in specific scenarios. However, a number of research initiatives have tackled the creation of generic communication frameworks to be used within the robot/WSN application domain.

Gil et al. [7] describes a data-centric middleware for wireless sensor networks in the scope of the European project AWARE. The middleware implements a high-level abstraction for integration of WSNs with mobile robots. This is achieved by providing data-centric access to the information gathered by the wireless sensor network, which includes mobile robotic nodes. Nodes in the network organize themselves to retrieve the information needed by the robots while minimizing the number of transmitted packets in order to save energy. Robots are connected via a high-bandwidth IEEE 802.11 WiFi network and interact with the low-bandwidth IEEE 802.15.4 WSN via a Gateway. The Gateway is in turn connected to both networks and used to collect the data gathered within the WSN.

The work of [8] focus in deploying mobile robots on environments already monitored by unstructured WSNs, for instance, in applications, such as search and rescue, where the robots must rely solely on this network for control and communication purposes. To this end, the mobile robots are equipped with sensor nodes and are capable of communicating with the WSN, which is used, not only to read WSN data, but also to access and control the robots. The resulting communication framework addresses bandwidth, message size and route restrictions by using adapter components to enable the communication of robot control messages through the WSN.

The RUBICON Communication Layer builds upon the PEIS middleware previously developed as part of the Ecologies of Physically Embedded Intelligent Systems project [PEIS] to provide a de-centralized mechanism for collaboration between separate processes running on separate devices. The PEIS middleware allows for automatic discovery, dynamic establishment of P2P networks, self-configuration and high-level collaboration in robotic ecologies through subscription–based connections and a tuplespace communication abstraction.

PEIS communicates by publishing information as tuples consisting of a <key, data> pair, together with various pieces of meta-information such as time-stamps, creator etc. Through a search mechanism, any PEIS can find and con-

 ISBN: 978-1-61208-231-8

sume the relevant tuples produced by any other PEIS, which allows for an expressive and flexible communication model. This tuple space thus constitutes a distributed database into which any PEIS-component can read and write information regarding any PEIS-component.

III. Communication Layer

The main objective of Communication Layer is to provide different type of communicating mechanisms for exchanging information between applications running on remote devices (robot, pc, motes, etc) of the Rubicon ecology. In particular, the Communication Layer will make available different paradigms of communication on the basis of the type of hardware involved in the communication, described by the following requirements.

A. Communication Requirements

- **Sensing**. In order to build and maintain an up-to-date picture of the state of the robotic ecology and its environment, and to enable collaboration between members of the robotic ecology (e.g. communication of localization data from the ceiling camera to the robot), the applications must be able to receive data and periodic status updates from every sensor and actuator it wishes for. In order to support reliability, the applications should also be able to specify the desired update rate and to be informed of the maximum latency to be expected by the resulting updates. The applications must tolerate the loss of some of these updates but all data must be time stamped in order to be able to ignore old updates.
- **Actuation**. The applications must be able to send control instructions (e.g. new set points, new output values) to every actuator it wishes for. For this type of transmission, the applications do not require the ability to communicate periodic updates of control instructions. However, in order to support reliability, transmission of control instructions should be reliable (acknowledged). In addition, the applications need to be informed of the maximum expected latency.
- **Data Sharing**. The applications must be able to (asynchronously) share it sensor data, actuator status and other information among distributed nodes (multiple robots, WSN nodes and other devices).
- **Messages**. In order to co-ordinate their operation across distributed nodes, the applications must be able to send reliable and synchronous control messages to all the nodes it wishes for.
- **Discovery**. The applications need an updated picture of all the components available in the system, including all the WSN nodes currently active. Every component should have a unique ID and the Control Layer should be informed whenever any robotic device or WSN nodes join (as they become operative and connect to the network), or leave the system (as they get disconnected, breaks, they battery get depleted or simply move out of network range

B. Architecture

In order to meet these requirements, the communication layer is mainly based on the two existing Software: the StreamSystem Middleware [9] and the PEIS Ecology middleware [10]. These two background technologies implement partly overlapping services but with important differences in hardware requirements and with services targeted towards applications for robotic devices and for distributed WSNs, respectively. The PEIS middleware provides automatic discovery, dynamic establishment of P2P networks, self-configuration and high-level collaboration in robotic ecologies through subscription–based connections and a *tuplespace* communication abstraction.

While the Tiny PEIS middleware kernel [11] is a specialization of the generic PEIS middleware to provide these high level robotic services also for WSN networks it requires significant WSN resources such as RAM memory and wireless bandwidth. Furthermore, due to the memory constraints and the single-hop only requirements of the Tiny PEIS on WSN nodes it is worthwhile to investigate a less restrictive approach for incorporating WSN nodes in the rich robotic middleware considered for the RUBICON project.

The Stream System framework provides a simple and effective access to the transducer and actuator hardware on wireless nodes, and a communication abstraction based on channels.

These two heterogeneous paradigms of communication are integrated by means of a star-topology (see Figure 1), in which a cluster of motes, called islands, will be interconnected by means of the PEIS-network. A special mote acting as sink node, connected via serial link with a *basestation* (a PC) will host a gateway component responsible for bridging the island with the tuplespace. In this way two basestations, which manage one island each, can communicate with each other through the PEIS middleware. By exploiting the P2P network of PEIS these devices can route messages originating in the islands to each other and forward such messages to the destination motes.

When a mobile robot comes within range of an island of motes, it can communicate with it through a local WSN mote carried by the robot capable of participating with the island as a peer and capable of forwarding messages and RSSI data to the robot. The sink node thus must be able to handle the dynamic connection and disconnection of a mobile robot mote. Furthermore the WSN must accommodate the possibility of more than one entry point of messages into / from the island. Note however that this does not pose any additional demands on the routing of outgoing message since any such messages can be propagated through the robot-based P2P network regardless of entry point.

 ISBN: 978-1-61208-231-8

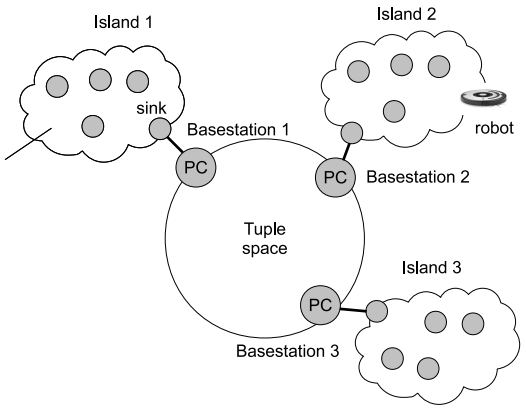


Figure 1. The Topology of the RUBICON Ecology

The communication layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. It controls the reliability of a given link through flow control, segmentation/desegmentation, and error control. Some protocols are state- and connection-oriented. This means that the communication layer can keep track of the segments and retransmit those that fail. It also provides the acknowledgement of the successful data transmission and sends the next data if no errors occurred.

IV. Integrating Robots and WSN

A. Architecture

The system is divided into two conceptual entities: the group Robot-Sink and the WSN deployed in the environment. The sink mote is connected to the Robot by means of a serial interface and acts as gateway between the Robot and the WSN. In particular, it forwards to the WSN the commands coming from the Robot and it notifies to the Robot the information coming from the WSN, for example the RSSI of the sensors or the detection of a particular event interesting for the Robot.

The Robot can move around in the environment according to the information coming from the WSN.

The part of the system running on each of the sensors of the WSN is composed of three layers (see Figure 4): Application, Transport and Network. The Application layer can be programmed according to the application requirements. In general, it receives the requests coming from the sink and reacts as consequence. For example it can respond to a request of reading one or more transducers value, or to a request to activate an actuator on the mote.

```
command error_t send(dest, data, nbytes,
    seq, comp_id);
event void receive(src, data, nbytes,
    seq, comp_id);
```

Figure 2. Network Layer Interface.

```
command error_t send(dest, data, nbytes,
    reliable, comp_id);
event void receive(src, data, nbytes,
    comp_id);
event void ack(seq, comp_id);
```

Figure 3. Transport Layer Interface.

B. Network layer

The Transport layer provides an interface for receiving messages to be sent over the radio and to signal the reception of incoming messages (see Figure 2). The textttsend command takes in input the destination address to send the message, the pointer to the data buffer to be sent, the number of bytes of the message, the sequence number of the message, and the identifier of the transport component that is sending the message. The `comp_id` parameter is used to perform the multiplexing/demultiplexing of the messages. In particular, it is used to deliver the message to the right component upon receiving a new message.

The address of mote in the Ecology is formed by the address of the island and the address of the mote in the island. The address of the island is a unique number that corresponds to the peis-id of the basestation. It is codified with a byte, that is interpreted as un unsigned integer. The value 255 is used to indicate “this-island”. The address of the mote is a two bytes unsigned integer and is a unique number that corresponds to the TinyOS-ID. The value 65535 is used to indicate a broadcast inside the island, and the value 65534 is used to indicate “myself”.

A robots that wants to join an island of the WSN, is equipped with a mote connected via USB to the Robot computing unit. The motes allows the robot to communicate either directly to any mote of the island or to the sync of the island.

C. The PEIS Proxy

To simplify the integration of application dependent objects into already deployed RUBICON ecologies, the communication layer will also exploit the concept of *PEIS proxy* [11]. This allows one to customize the available hardware devices without any need for re-implementation of any of the robotic software already running in the ecology.

For each island node, the basestation creates a PEIS proxy component that emulates the behavior of the WSN mote. This proxy component is characterized by (a) appearing as a unique entity with a unique ID number in the PEIS ecology

 ISBN: 978-1-61208-231-8

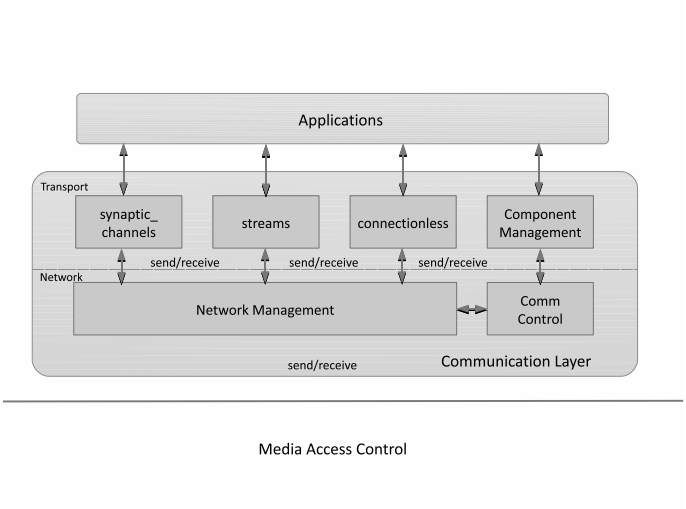


Figure 4. The architecture of the Communication Layer

and (b) it publishes and receives tuple data corresponding to the operations available to all WSN motes.

Initially this PEIS proxy node is populated by the basestation with all statistic information about the given node, relying on a static translation between the mote type and the functionalities that the gateway associated with mote type.

Whenever the WSN basestation receives updated sensor data from a mote, it translates these sensor data to the format of the PEIS tuplespace (most notably, in ascii format) and publishes it to the corresponding WSN proxy node. Furthermore, it subscribes to changes to any actuation tuples in the proxy node, and translates and sends actuation commands to the corresponding mote.

If multiple basestations are in range of the same mote, a failure is noted when they attempt to create the proxy for each node. This failure to create an additional node is regulated in the basic PEIS ecology framework and will lead to only one of the two basestation to be able to proxy the same WSN node.

D. Transport layer

The Transport layer provides a first abstraction for sending the messages (see Figure 3). In particular, it keeps track of the pending messages (by means of a sequence number that it adds to each message to be sent), it provides the feature of a reliable communication and it manages the ack of the reliable messages. It may offer additional services, such as connection-oriented service. In this case it is the responsible for allocating the data structures needed to the communication and to maintain them.

Here is a list of features that the communication layer provides to the WSN developers:

- *Synaptic Communication*: This type of communication is used exclusively by the Learning Layer and enables two ESNs (Echo State Network), running on different nodes, to exchange data. In particular it enables the transmission of the output of a set of neurons from a source ESN to a destination ESN.
- *Data Stream Communication*: This type of communication is used exclusively by the Control Layer and enables the point-to-point communication between two specific devices, typically for reading data from remote mote transducers.
- *Connectionless Message Passing*: This type of communication is used exclusively by the Control Layer and enables the point-to-point communication between two specific devices, typically for sending commands to remote mote-actuators.

Data Stream Communication is the paradigm of communication more relevant for the purposes of integration between robots and WSN. The stream represents a generic unidirectional data channel that is able to carry data records. In particular, we have three types of streams:

1) **Local Streams** represent local data channels where read and write operations must occur on the hosting sensor.
2) **Sensor Streams** are the basic abstraction for collecting readings from transducers. They can only be read by operators since the writing is carried out by the associated transducers (these can be thought of as virtual operators writing to sensor streams).
3) **Remote streams** require cooperation between two nodes since they intend to provide a data channel between two different nodes. Write operations can be carried out on one of them (the stream write-end) and read operations can take place on the other (the read-end).

Figure 5 illustrates these concepts.

Another important concept in command/event-based systems is that of split-phase operations. The call requesting to start the operation returns immediately, without waiting for the operation to complete.

V. Conclusion and Future Work

The purpose of the RUBICON project is to create a robotic ecology comprising robots, a large number of heterogeneous environmental sensors and actuators, and learning and cognitive capabilities. In this ecology, the communication layer should provide almost homogeneous services to devices with very different communication and processing capacities. The approach chosen in RUBICON is to build communication services on top of established robotic and WSN middlewares.

This paper draws the status of the development of the communication layer, which is still in the early stage of development. In particular, based on the RUBICON communication requirements, it describes the overall architecture of

 ISBN: 978-1-61208-231-8

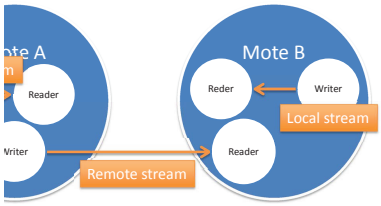


Figure 5. The paradigm of the data stream communication

the communication layer and its current status of development, and it discusses how the integration ROBOTS-WSN is achieved.

Next steps of the RUBICON communication layer developments, which will span the next 18 months, are the integration of specific communication mechanisms for connecting the RUBICON distributed learning and cognitive components, and its validation and performance evaluation.

One of the scenarios that we are going to test will exploit a data acquisition application that can be used by mobile robots to acquire sensor and radio signal strength index (RSSI) information to support their localization in indoor environments.

ACKNOWLEDGMENT

This work has been partially supported by the EU FP7 RUBICON project (contract n. 269914).

REFERENCES

[1] T.-C. Chen, T.-S. Chen, and P.-W. Wu, "On data collection using mobile robot in wireless sensor networks," *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, vol. 41, no. 6, pp. 1213 –1224, nov. 2011.

[2] M. Rahimi, H. Shah, G. Sukhatme, J. Heideman, and D. Estrin, "Studying the feasibility of energy harvesting in a mobile sensor network," in *Robotics and Automation, 2003. Proceedings. ICRA '03. IEEE International Conference on*, vol. 1, sept. 2003, pp. 19–24.

[3] A. LaMarca, W. Brunette, D. Koizumi, M. Lease, S. Sigurdsson, K. Sikorski, D. Fox, and G. Borriello, "Making sensor networks practical with robots," in *Pervasive Computing*, ser. Lecture Notes in Computer Science, F. Mattern and M. Naghshineh, Eds. Springer Berlin / Heidelberg, 2002, vol. 2414, pp. 615–622.

[4] E. Menegatti, A. Zanella, S. Zilli, F. Zorzi, and E. Pagello, "Range-only slam with a mobile robot and a wireless sensor networks," in *Robotics and Automation, 2009. ICRA '09. IEEE International Conference on*, may 2009, pp. 8 –14.

[5] G. Tuna, K. Gulez, and V. Gungor, "Communication related design considerations of wsn-aided multi-robot slam," in *Mechatronics (ICM), 2011 IEEE International Conference on*, april 2011, pp. 493 –498.

[6] M. A. Batalin, "Symbiosis: cooperative algorithms for mobile robots and a sensor network," Ph.D. dissertation, Los Angeles, CA, USA, 2005, aAI3180329.

[7] P. Gil, I. Maza, A. Ollero, and P. J. Marron, "Data centric middleware for the integration of wireless sensor networks and mobile robots," in *Proceedings of the 7th Conference On Mobile Robots And Competitions*, Paderne, Portugal, 2007.

[8] L. de Souza, R. Padilha, and C. Decker, "Neural fault isolator for wireless sensor networks," in *Networked Sensing Systems, 2008. INSS 2008. 5th International Conference on*, june 2008, pp. 47 –50.

[9] G. Amato, S. Chessa, and C. Vairo, "Mad-wise: A distributed stream management system for wireless sensor networks," in *Software Practice & Experience, 40 (5): 431 - 451*, 2010.

[10] M. Broxvall, "A middleware for ecologies of robotic devices," in *Proceedings of the 1st international conference on Robot communication and coordination*, ser. RoboComm '07. Piscataway, NJ, USA: IEEE Press, 2007, pp. 30:1–30:8.

[11] M. Bordignon, J. Rashid, M. Broxvall, and A. Saffiotti, "Seamless integration of robots and tiny embedded devices in a peis-ecology," in *Proc of the IEEE/RSJ Int Conf on Intelligent Robots and Systems (IROS)*, San Diego, CA, 2007, pp. 3101–3106.

 ISBN: 978-1-61208-231-8

A Communication and Localization Framework Suited for Nomadic Wireless Sensor Networks

Luca Bencini
Dept. of Innovation & Technology
T.T. Tecnosistemi S.p.A.
Via Rimini 5, 59100 Prato, Italy
Luca.Bencini@tecnosistemi.com

Stefano Maddio
Dept. of Electronics and Telecommunication
University of Florence
Via di Santa Marta 3, 50139 Florence, Italy
stefano.maddio@unifi.it

***Abstract*—In this paper, an energy efficient communication and localization framework able to manage the synchronization between nodes and to provide the localization of nomadic nodes within Nomadic Wireless Sensor Networks is presented. It is comprised of a MAC protocol based on sleep and active states and a novel localization algorithm based on Differential Direction of Arrival. Some numerical simulations was performed to show the low power consumption of the proposed protocol. Moreover, a system of fixed and nomadic nodes was implemented to test the proposed localization algorithm. The reported experiments show a mean positioning error of 0.61 m and a mean orientation error of 17 degrees within a 10 m x 10 m square space.**

***Keywords*-Wireless Sensor Network; Energy Efficient Protocol; Differential Direction of Arrival; Switched Beam Antenna.**

I. INTRODUCTION

The management of mobility within Wireless Sensor Networks [1] (WSNs) has recently gained much interest as the number of applications that require nomadic sensor nodes has increased. The presence of nomadic nodes within a WSN allows the improvement of system monitoring capabilities but, at the same time, it increases the system complexity (since a localization algorithm is required), the energy consumption, as well as the delay and the latency of the network. For this purpose, adopting a nomadic WSN is expected to satisfy calls for a carefully localization algorithm and an optimized communication protocol able not only to minimize the energy waste, but also to synchronize the fixed and the nomadic nodes and to manage the localization procedure.

This paper deals with a communication and localization framework suitable for Nomadic WSN. In particular, after a brief description of the 2D Music algorithm, the proposed localization algorithm is presented in in Section III. In Section IV, the communication protocol is described. Finally, in Sections V and VI, protocol performance and some localization tests are reported.

II. 2-D MUSIC ALGORITHM

Let an array of N omnidirectional elements receive signals from L ($L < N$) narrowband far-field sources with the unknown Direction of Arrivals (DOAs) $\{\phi_1, \ldots, \phi_L\}$. The array $N \times 1$ snapshot vector at time k can be modeled as [2]

$$x(k) = A(\phi)s(k) + n(k) \tag{1}$$

where $\phi = [\phi_1, \ldots, \phi_L]^T$ is the $L \times 1$ vector of signal DOAs,

$$A(\phi) \doteq [a(\phi_1), \ldots, a(\phi_L)] \tag{2}$$

is the $N \times L$ signal steering matrix, $s(k)$ is the $L \times 1$ vector of signal waveforms, $n(k)$ is the $N \times 1$ vector of noise and $(\cdot)^T$ stands for the transpose.

Assuming an array of arbitrary geometry, the $N \times 1$ steering vector can be expressed as

$$a(\phi) = \left[\ldots, e^{j\frac{2\pi}{\lambda}(x_i sin\phi + y_i cos\phi)}, \ldots\right]^T \tag{3}$$

where λ is the signal wavelength, $j = \sqrt{-1}$, $\{x_i, y_i\}$ $(i = 1, \ldots, N)$ are the coordinates of the ith array element and and it will be hereafter assumed that the array manifold is known exactly.

The $N \times N$ array covariance matrix can be written as

$$R_x \doteq E\{x(k)x^H(k)\} = AR_sA^H + \sigma_n^2 I \tag{4}$$

where $R_s = E\{s(k)s^H(k)\}$ is the source covariance matrix, σ_n^2 is the noise variance, I is the identity matrix, $E(\cdot)$ is the statistical expectation and $(\cdot)^H$ is the Hermitian transpose (transpose and conjugate of $(\cdot)$).

The singular value decomposition of the exact covariance matrix can be written as

$$R_x = \sum_{k=1}^{N} \lambda_k u_k u_k^H \tag{5}$$

where λ_k and u_k $(k = 1, \ldots, N)$ are the singular values and corresponding singular vectors. Let the singular values λ_k be sorted in nonascending order. Then, the matrices

$$U_s \doteq [u_1, \cdots, u_L], \qquad U_n \doteq [u_{L+1}, \cdots, u_N] \tag{6}$$

 ISBN: 978-1-61208-231-8

contain L the signal and $N - L$ noise subspace singular vectors, respectively.

In practical situations, the exact array covariance matrix R_x is unavailable and its sample estimate

$$\hat{R}_x = \frac{1}{K}\sum_{k=1}^{K} x(k)x^H(k) \tag{7}$$

is used, where K is the number of snapshots.

The singular value decomposition of the sample covariance matrix (7) yields

$$\hat{R}_x = \hat{U}_s\hat{\Lambda}_s\hat{U}_s^H + \hat{U}_n\hat{\Lambda}_n\hat{U}_n^H \tag{8}$$

where the sample singular values are again sorted in nonascending order ($\hat{\lambda}_1 \geq \hat{\lambda}_2 \geq \cdots \geq \hat{\lambda}_N$) and the matrices $\hat{U}_s \doteq [\hat{u}_1, \ldots, \hat{u}_L]$ and $\hat{U}_n \doteq [\hat{u}_{L+1}, \ldots, \hat{u}_N]$ contain in their columns the signal and noise subspace singular vectors of $\hat{R}_x$, respectively. Correspondingly, the diagonal matrices $\hat{\Lambda}_s \doteq diag\{\hat{\lambda}_1, \ldots, \hat{\lambda}_L\}$ and $\hat{\Lambda}_n \doteq diag\{\hat{\lambda}_{L+1}, \ldots, \hat{\lambda}_N\}$ are built from the signal and noise subspace singular values of $\hat{R}_x$, respectively.

The conventional MUSIC null-spectrum function can be expressed as

$$f(\phi) = a^H(\phi)\hat{U}_n\hat{U}_n^H a(\phi) = \|\hat{U}_n^H a(\phi)\|^2 \tag{9}$$

where $\|\cdot\|^2$ is the vector 2-norm. The spectral MUSIC technique estimates the signal DOAs from the minima of this function by searching over ϕ with a fine grid. The computational complexity of this spectral search step is typically substantially higher than that of the singular value decomposition step because, as a rule, $J \gg N$ where J is the total number of spectral points. Note that for each spectral point, the product of $\hat{U}_n^H$ and $a(\phi)$ (or, alternatively of $\hat{U}_s$ and $a(\phi)$) has to be computed.

Often, the inverse of the normalized MUSIC null-spectrum function is considered to compute and exalt the signal DOAs. This function is computed as follow.

$$f(\phi) = \frac{\|a(\phi)\|}{\|\hat{U}_n^H a(\phi)\|^2} \tag{10}$$

In this case the signal DOAs is estimated from the maxima of (10).

III. Localization Algorithm

Let A, B and C be three *fixed nodes* positioned in a Euclidean Geometry Plane Π and having coordinates (x_A, y_A), (x_B, y_B) and (x_C, y_C), respectively.

Let M be a *nomadic node* also positioned in the plane Π and having generic coordinates (x_M, y_M). M is equipped by a Switched Beam Antenna characterized by a group of N directive antennas that together cover an angle of 360°. Let $a_i(\phi)$ $(i = 1, \ldots, N)$ be the azimuth steering vector (gain vector) of each directive antenna.

M computes its coordinates (x_M, y_M) in three steps.

1) It applies the MUSIC algorithm.
2) It applies the law of sines starting from the knowledge of the coordinates of the fixed nodes.
3) It performs the trilateration algorithm.

A. MUSIC algorithm

According to (1) and (7), M builds up for each fixed nodes K vectors of $N \times 1$ RSSI values. Let $x_{k0_i}(\cdot)$ $(k0 \in [1; K])$ the k^{th} RSSI vector of the fixed node i $(i = A, B, C)$. The position $x_{k0_i}(n0)$ $(n0 \in [1; N] \wedge k0 \in [1; K])$ will contain the RSSI value computed at the k^{th} iteration selecting the n^{th} antenna's sector. The RSSI values can also be organized in matrix form as follow.

$$X_i = \begin{pmatrix} x_{11_i} & \cdots & x_{1K_i} \\ x_{21_i} & \cdots & x_{2K_i} \\ \vdots & \ddots & \vdots \\ x_{N1_i} & \cdots & x_{NK_i} \end{pmatrix} \tag{11}$$

Then, according to (7) and (8), M computes for each fixed node the covariance matrix R_{x_i} $(i = A, B, C)$ as

$$\begin{aligned} R_{x_i} &= \tfrac{1}{K}\sum_{k=1}^{K} x_{k_i}(n)x_{k_i}^H(n) \\ &= U_{s_i}\Lambda_{s_i}U_{s_i}^H + U_{n_i}\Lambda_{n_i}U_{n_i}^H \end{aligned} \tag{12}$$

Finally, according to (10), M evaluates the angles ϕ_i $(i = A, B, C)$ as

$$\phi_i = argmax_\phi \frac{a(\phi)}{a^t(\phi)U_{n_i}U_{n_i}^t a(\phi)} \tag{13}$$

B. Law of Sine

Let a, b and c be the lengths of the legs of a triangle opposite angles $\hat{A}$, $\hat{B}$ and $\hat{C}$. Then the law of sines states that

$$\frac{a}{\sin\hat{A}} = \frac{b}{\sin\hat{B}} = \frac{c}{\sin\hat{C}}$$

If two sides of a triangle are the radius, the law of sines states that

$$|\overline{AB}| = 2R\sin(\frac{\phi_C}{2}) \tag{14}$$

where, as Figure 1 shows, $\overline{AB}$ is a chord, R is the radius of the circle and finally ϕ_C is the angle at the centre subtended by the chord $\overline{AB}$. Knowing also that:

1) angles at the circumnference subtended by a chord in the same segment are equal and
2) if two angles stand on the same chord, then the angle at the centre is twice the angle at the circumnference,

Equation (14) can be expressed as

$$|\overline{AB}| = 2R\sin(\phi_{AB}) \tag{15}$$

The law of sines is used by the nomadic node M to perform another step towards the evaluation of its position. From the knowledge of the coordinates of the anchor nodes

 ISBN: 978-1-61208-231-8

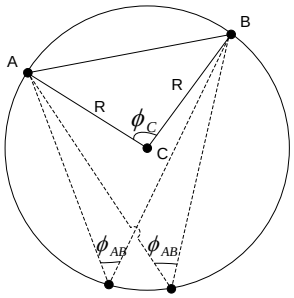


Figure 1: Specific application of law of sines

and the angles ϕ_A, ϕ_B and ϕ_C, M obtains the equation of three circumferences $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ passing for M and for A and B, B and C and C and A, rispectively. The equations can be expressed as follow:

$$\begin{aligned}
\mathcal{A}: \quad & (x-x_{\mathcal{A}})^2+(y-y_{\mathcal{A}})^2 = \tfrac{(x_B-x_A)^2+(y_B-y_A)^2}{2\sin\hat{\phi}_{AB}} \\
\mathcal{B}: \quad & (x-x_{\mathcal{B}})^2+(y-y_{\mathcal{B}})^2 = \tfrac{(x_C-x_B)^2+(y_C-y_B)^2}{2\sin\hat{\phi}_{BC}} \\
\mathcal{C}: \quad & (x-x_{\mathcal{C}})^2+(y-y_{\mathcal{C}})^2 = \tfrac{(x_A-x_C)^2+(y_A-y_C)^2}{2\sin\hat{\phi}_{CA}}
\end{aligned}$$

where

$$\begin{aligned}
(x_{\mathcal{A}}, y_{\mathcal{A}}) &= \tfrac{1}{2}(x_A+x_B, y_A+y_B)+ \\
&+ \tfrac{1}{2}(y_A-y_B, -x_A+x_B)\cot\hat{\phi}_{AB} \\
(x_{\mathcal{B}}, y_{\mathcal{B}}) &= \tfrac{1}{2}(x_B+x_C, y_B+y_C)+ \\
&+ \tfrac{1}{2}(y_B-y_C, -x_B+x_C)\cot\hat{\phi}_{BC} \\
(x_{\mathcal{C}}, y_{\mathcal{C}}) &= \tfrac{1}{2}(x_C+x_A, y_C+y_A)+ \\
&+ \tfrac{1}{2}(y_C-y_A, -x_C+x_A)\cot\hat{\phi}_{CA}
\end{aligned}$$

are the centers of the circles and $\hat{\phi}_{AB}$, $\hat{\phi}_{BC}$ and $\hat{\phi}_{CA}$ are $\hat{\phi}_A-\hat{\phi}_B$, $\hat{\phi}_B-\hat{\phi}_C$ and $\hat{\phi}_C-\hat{\phi}_A$.

C. Trilateration Algorithm

Finally, M finds its position performing the trilateration. In particular, it finds the intersection point of the cirmunferences $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$. This concept is shown in Figure 2.

The intersection point is simple to compute thanks to the following formulas:

$$\begin{aligned}
x &= x_{\mathcal{A}} + \tfrac{d_x k}{p} + \tfrac{d_y}{p}\sqrt{r_{\mathcal{A}}^2-k^2} \\
y &= y_{\mathcal{A}} + \tfrac{d_y k}{p} - \tfrac{d_x}{p}\sqrt{r_{\mathcal{A}}^2-k^2}
\end{aligned}$$

where $d_x = x_{\mathcal{A}} - x_{\mathcal{B}}$, $d_y = y_{\mathcal{A}} - y_{\mathcal{B}}$, $p = \sqrt{d_x^2+d_y^2}$ and $k = \frac{p^2+r_{\mathcal{A}}^2-r_{\mathcal{B}}^2}{2p}$.

Once the position of the nomadic node is estimated, the orientation is determined in a straigh-forward manner. Given the position, the angle between the nomadic node and one of the anchor is easily derived as

$$\theta_B = \frac{x_M - x_B}{y_M - y_B}$$

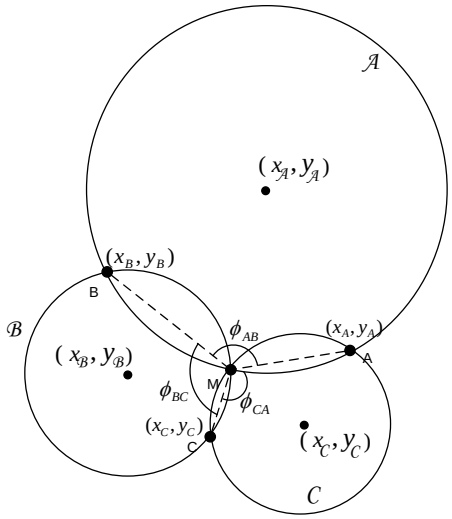


Figure 2: Trilateration

The nomadic node orientation is simply estimated as

$$\psi = \theta_B - \phi_B$$

IV. MAC Protocol

Taking the IEEE 802.11 Distributed Coordination Function (DCF) [3] as a starting point, several more energy efficient techniques have been proposed in literature to avoid excessive power waste due to so called idle listening. They are based on periodical preamble sampling performed at the receiver side in order to leave a low power state and receive the incoming messages, as in the WiseMAC protocol [4]. Deriving from the classical contention-based scheme, several protocols (S-MAC [5] and TMAC) have been proposed to address the overhead idle listening by synchronizing the nodes and implementing a duty cycle within each slot.

Resorting to the above considerations, a class of MAC protocols was derived, named *Synchronous Transmission Asynchronous Reception* (STAR) which is particularly suited for a flat network topology and benefits from both WiseMAC and S-MAC schemes. More specifically, due to the introduction of a duty-cycle, it joins the power saving capability together with the advantages provided by the offset scheduling, without excessive overhead signaling.

According to STAR protocol, each node wakes up independently, entering an initial idle state (*init state*) in which it remains for the time interval necessary for performing the elementary CPU operations and to be completely switched on (T_{init}). Moreover, before entering the *discovery state*, each device starts to organize the time into frames whose durations are T_f.

In the *discovery state*, each node tries to identify its neighbors and to establish a time synchronization with them. To this purpose, it remains in a listening mode for a time interval equal to $T_{set-up} \geq 2T_f$ and begins to periodically

broadcast a HELLO message sending its *ID* and its *phase*. The phase is the time interval after which the sender exits from the *discovery state*, enters the regime state and changes back in listening mode. A node that receives a HELLO message adds the source node to the list of its own active neighbors and transmits an acknowledgement.

Once the *discovery state* has expired, each node enters the *regime state*. Within this state, the operation mode is duty cycled with a periodic alternation of listening and sleeping sub-periods whose time intervals are T_l and T_s, respectively. The duty cycle function is given by the following formula:

$$d = \frac{T_l}{T_l + T_s} \tag{16}$$

In the *regime state*, each node tries to preserve the synchronization with its neighbors. To achieve this, it sends a frame-by-frame HELLO message in a unicast way to the active nodes in its list according to the phase transmitted by them in previous HELLO messages. As in the *discovery state*, the HELLO message contains the *ID* and the *phase* that, in this case, is the time interval after which the sender claims to be again in the listening status waiting for the HELLO messages. The phase ϕ is evaluated according to the following rule:

$$\phi_1 = \tau - T_l \tag{17}$$

if the node is in the sleeping mode, where τ is the time remaining to the beginning of the next frame. Conversely, if the node is in the listening status, ϕ_2 is computed as:

$$\phi_2 = \tau + T_s \tag{18}$$

In the *regime state*, nomadic nodes are able to move within the operative area. Unlike the fixed nodes equipped by an omnidirectional antenna, they are hardwired with a *Switched Beam Antenna*, a group of N overlapping adjacent beams (sectors) that together cover an angle of $360°$. When a nomadic node reaches its intermediate waypoint, it stops for a predefined pause time (T_{pt}) and broadcasts a HELLO message per sector for a time interval equal to $2T_f$ by notifying its presence and listening the channel in search of HELLO messages sent by the fixed nodes in its coverage area. At the end of the scanning, if the nomadic node found a number of active fixed nodes less than three, it moves itself; otherwise it groups the fixed nodes per sector and chooses the three nodes with the hightest RSSI value and belonging to different sectors (preferably opposite sectors). If this choice is not possible, it takes into account only the three nodes with the hightest RSSI value.

According to the *phase* stored during the scanning interval, the nomadic node sends a LOCALIZATION REQUEST message to the first fixed node. The fixed node wakes up and sends k ($k/N \in \mathbb{N}^+$) LOCALIZATION RESPONSE messages thanks to which the nomadic node creates a $k/N \times N$ matrix of RSSI values.

The nomadic node performs the same procedure to the other two fixed nodes.

Finally, it applies the localization algorithm described in Section III to evaluate its position within the operative area.

Once T_{pt} is expired, it keeps moving again.

The channel access is managed by means of the carrier sense multiple access with collision avoidance (CSMA/CA) scheme. This mechanism is very effective in reducing collisions.

Each node remains in the *regime state* until there is at least one neighbor, otherwise if there are no active neighbors it reenters the *discovery state* in search of connectivity.

To complete the protocol characterization, whenever a node battery is depleted, this node turns off, entering an *off state*.

V. Protocol Performance Analysis

In order to fully characterize the STAR MAC approach, the related energy cost normalized can be evaluated, as follows:

$$C = c_{rx} d T_f + c_{sleep}[T_f(1-d) - NT_{pkt}] + NC_{tx} \quad [mAh] \tag{19}$$

where c_{sleep} and c_{rx} represent the sleeping and the receiving costs $[mA]$ and C_{tx} is the single packet transmission costs $[mAh]$, T_f is the frame interval $[s]$, d is the duty cycle, T_{pkt} is the synchronization packet time length $[s]$ and finally N is the number of neighbors. When the following inequality holds:

$$NT_{pkt} \ll T_f \tag{20}$$

then:

$$C \simeq c_{rx} d T_f + c_{sleep} T_f (1-d) + NC_{tx} \quad [mAh] \tag{21}$$

The protocol cost normalized to the synchronization time is finally:

$$\frac{C}{T_f} = c_{rx} d + c_{sleep}(1-d) + \frac{NC_{tx}}{Tf} \quad [mA] \tag{22}$$

As highlighted in TABLE I, it usually happens that $c_{tx} \ll c_{sleep} \ll c_{rx}$, where $c_{tx} = C_{tx}/T_{pkt}$ and T_{pkt} is the packet transmission time $[s]$ assumed equal to $100\ ms$ as worst case. This means that the major contribution to the overall cost is represented by the listening period that the STAR MAC protocol tries to suitably minimize.

TABLE I: POWER CONSUMPTION PARAMETERS FOR THE CONSIDERED PLATFORM

c_{rx}	$12 \quad mA$
c_{sleep}	$0.01 \quad mA$
C_{tx}	$30 \quad mAh$
c_{tx}	$0.001 \quad mA$

In Figure 3(a), the normalized cost versus the number of neighbor nodes is shown for the S-MAC and STAR

 ISBN: 978-1-61208-231-8

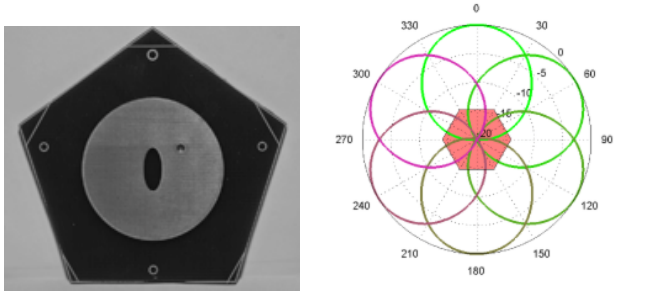
MAC schemes. It is worth noticing that the performance of the proposed protocol is better with respect to the existing approach for a number of neighbor nodes greater than 7. In Figure 3(b), the normalized costs of S-MAC and STAR MAC approaches are compared with respect to the duty cycle duration for a number of neighbor nodes equal to 8. It is possible to notice that for $d < 3.5\%$ the proposed protocol provide a significant gain.

VI. Experimental Localization Results

In this section, some experimental results are presented.

The experiments were conducted in a room of $10m \times 10m$. Fixed nodes assumed the following positions: $A = (1.25, 1.78)\ m$, $B = (8.66, 1.81)\ m$ and $C = (4.50, 8.50)\ m$, respectively. This arrangement resambles an almost equilateral triangle, a suited shape to uniformly covers the test area. Otherwise nomadic node assumed four position $P_1 = (4.50, 4.72)$; $P_2 = (2.85, 4.72)$, $P_3 = (6.20, 4.72)$, $P4 = (4.50, 5.50)$. The nomadic node reference was always parallel to the positive x axis, i.e it faces the east direction.

Both fixed and nomadic nodes were able to scan signals in a emphomnidirectional manner (in a 2D sense), but in a different sense. The fixed nodes were equipped with a common dipole, a standard low-gain omnidirectional radiator. The nomadic node instead was equipped with a Switched Beam Antenna (SBA).



(a) Antenna Element

(b) Pictorial Representation of the 6 Patterns

Figure 4: Switching beam system. Given the antenna pattern, a six elements arrangement is enough to cover the entire angular range.

To keep a cost-effective profile, this array is made of 6 printed antennas working at $2.45\ GHz$ directly fed by a commercial single pole six through (SP6T) FET switch. The natural arrangement to cover the entire 2π angular range is the uniform circular array (UCA). This structure is the best trade-off between the need of simple architecture for and a wide angle steerable beam. The SBA gain G can be represented by six element vectors. This structure is the best trade-off between the need of a simple architecture and a wide angle steerable beam. The elementary patch antenna of the array shown in Figure 4 is an Elliptical Slitted Disc Antenna [6], a circularly polarized radiator well suited for localization purposes. Printed on a cheap plastic substrate ($\varepsilon_r = 4.4$, $h = 1.6\ mm$), the antenna shows a cardioid-like pattern, suitable for the switched beam arrangement. The compact dimension of $35\ mm$ is a good compromise between CP radiations and pattern degradation by electromagnetic coupling.

The results of the four experiments are depicted in Figure 5 and Figure 6. In all the cases, the radial error was below $90\ cm$, and the orientation of the system was identified within the $35°$ of pointing error. The entire experimental data set showed an average error in the position estimation of $0.61\ m$ and $17°$ for the orientation.

VII. Conclusion and Future Work

The management of mobility within WSNs has recently gained much interest as the number of applications that require nomadic sensor nodes has increased. The presence of nomadic nodes within a WSN allows the improvement of system monitoring capabilities but, at the same time, it increases the system complexity (since a localization algorithm is required), the energy consumption, as well as the delay and the latency of the network.

In this paper, a communication and localization framework was proposed. The numerical and experimental results showed the advantages and the feasibility of the proposed solution. This allows the application of the solution under investigation to the more general field of environmental monitoring and in particular in robot applications.

Acknowledgment

The authors would like to thank T.T. Tecnosistemi S.p.A.

References

[1] J. Yick, B. Mukherjee and D. Ghosal, *Wireless sensor network survey*, in Journal on Computer Network, Vol. 52, pp. 2292-2330, April 2008.

[2] R.O. Schmidt, *Multiple Emitter Location and Signal Parameter Estimation*, in IEEE Transaction on Antennas and Propagation, Vol. 34, pp. 276-280, March 1979.

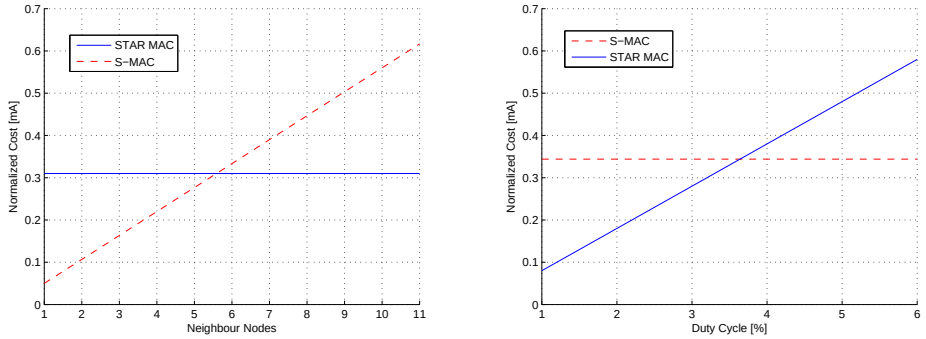
[3] I. of Electrical and E. Engineers, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard 802.11-1997, New York, NY, 1997.

[4] A. El-Hoiydi, J. Decotignie, C. Enz, and E. Le Roux, *WiseMAC, an Ultra Low Power MAC Protocol for the WiseNET Wireless Sensor Network*, in Proc. of SENSYS 2003, Vol. 1, pp. 244-251, November 2003.

[5] W. Ye, J. Heidemann, and D. Estrin, *An Energy-Efficient MAC Protocol for Wireless Sensor Networks*, in Proc. of INFOCOM 2002, vol. 3, pp. 1567-1576 June 2002.

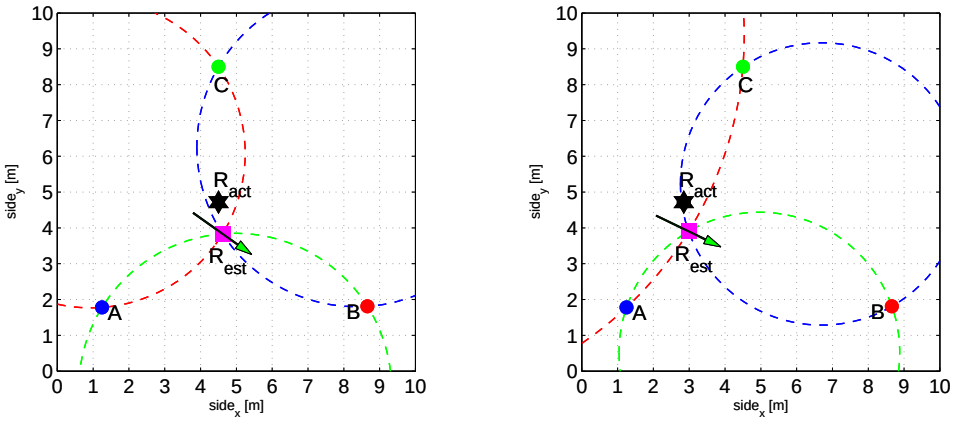
[6] S. Maddio, A. Cidronali and G. Manes, *A New Design Method for Single-Feed Circular Polarization Microstrip Antenna with an Arbitrary Impedance Matching Condition*, in IEEE Transactions on Antennas and Propagation, 2010.

 ISBN: 978-1-61208-231-8



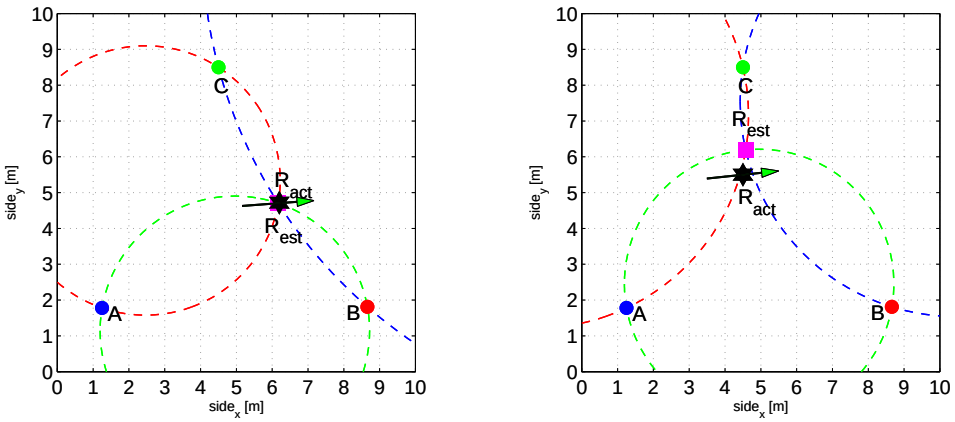
(a) Normalized Cost vs. Neighbor Nodes (b) Normalized Cost vs. Duty Cycle Duration

Figure 3: STAR MAC Performance



(a) experiment #1: actual position: $(\hat{x}, \hat{y}) = (4.50, 4.72)$, $err_{xy} = (0.11, -0.88)$, $err_{tot} = 0.89$, $ori_{err} = -35$ (b) experiment #2: actual position: $(\hat{x}, \hat{y}) = (2.85, 4.72)$, $err_{xy} = (0.13, -0.81)$, $err_{tot} = 0.82$, $ori_{err} = -25$

Figure 5: The first two experiments. The hexa-star is the actual position of the nomadic node (indicated with R), while the square is the estimated position and arrow indicates the estimated orientation.



(a) experiment #3: actual position: $(\hat{x}, \hat{y}) = (6.20, 4.72)$, $err_{xy} = (-0.03, -0.01)$, $err_{tot} = 0.03$, $ori_{err} = 4$ (b) experiment #4: actual position: $(\hat{x}, \hat{y}) = (4.50, 5.50)$, $err_{xy} = (0.08, 0.69)$, $err_{tot} = 0.69$, $ori_{err} = 6$

Figure 6: The second two experiments. The hexa-star is the actual position of the nomadic node (indicated with R), while the square is the estimated position and arrow indicates the estimated orientation.

 ISBN: 978-1-61208-231-8

JAFSPOT: Java Agent-Based Framework for Sun SPOT Wireless Sensor Networks

Hakan Cam, Ozgur Koray Sahingoz
Computer Engineering Department
Turkish Air Force Academy
Istanbul, Turkey
{h.cam, sahingoz}@hho.edu.tr

Ahmet Coskun Sonmez
Computer Engineering Department
Yildiz Technical University
Istanbul, Turkey
acsonmez@ce.yildiz.edu.tr

***Abstract*—Due to increasing capabilities of micro-sensors, wireless sensor networks have emerged as one of the key growth areas in recent years. They are a collection of sensor nodes deployed over a target region for observing physical phenomena, such as temperature, light, accelerometer, etc. Mobile agent model is a distributed computing paradigm, which is capable of solving problems effectively in dynamic and open environments like wireless sensor networks. Few mobile agent systems have been developed for wireless sensor networks so far. In this paper, we describe JAFSPOT, a Java Agent-based Framework for Sun SPOT. It uses event-based programming in which the core components communicate through events. To the best of our knowledge, JAFSPOT is one of the very few mobile agent-based frameworks for wireless sensor networks that support migration of isolates. First, we describe the core components of the proposed system, then present a sample application about monitoring Sun SPOT sensor node with mobile agents and finally, give the results of an experiment to evaluate the performance of this system in terms of time and energy consumption.**

Keywords- Wireless Sensor Networks; Mobile Agent Systems.

I. INTRODUCTION

Depending on recent developments in processing, power, storage, micro-sensor and wireless communication technologies, Wireless Sensor Networks (WSNs) have become a broad area of interest in military, academic and industrial circles [1]. WSNs are composed of hundreds of sensor devices coming together and communicating over a wireless radio. These sensor devices are low cost, tiny devices with low power, constrained storage, limited processing and short-range wireless communication capabilities [2]. A sample WSN architecture is depicted in Figure 1.

The mobile agent (MA) paradigm is a distributed computing mechanism used for remedying the problems of dynamically changing environments, such as WSNs. It is a software process that can operate autonomously and can migrate to its code and state. It provides a way to dynamic reprogramming and facilitates a powerful and flexible mechanism for complex distributed problems of WSN systems [3][4].

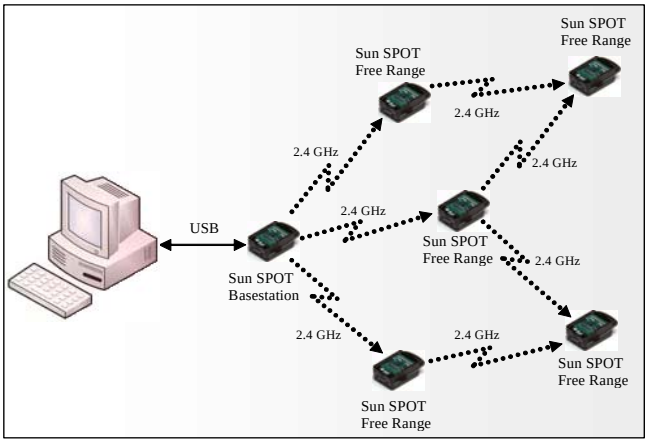


Figure 1. Wireless sensor network architecture

Since MAs can provide some reasonable, practical and inexpensive solutions for the WSNs limitations, integration of WSNs with MAs is emerging as an essential requirement. Some of the limitations of WSNs are: energy for long network lifetime, restricted bandwidth for wireless communication, hardware due to the small size of the sensor nodes, unstable network connections due to the mobility and lifetime of the sensor nodes, low-level re-programmability due to its distributed structure. Due to these constraints, deploying a new code into a distributed WSN and upgrading it is an extremely cumbersome issue. In addition to these constraints, while most WSNs have typically been developed in an application-specific manner, sensor devices can store and run multiple applications at the same time. Instead of storing and running all applications in a single sensor device, using of MAs seems to be a more practical solution [5]. MA paradigm is a way of smart programming and can be regarded as the further development of a distributed problem-solving of WSNs [6]. Performance of WSNs can be improved by using MAs via improving communication and coordination capabilities. A sample MA-based WSN structure is depicted in Figure 2.

WSNs can benefit from MAs in several ways: First, MAs use the bandwidth more efficiently by transferring its code to the interested target area. Therefore, there is no need to circulate the raw data over the network. Second, MAs provide effective and dynamic re-

 ISBN: 978-1-61208-231-8

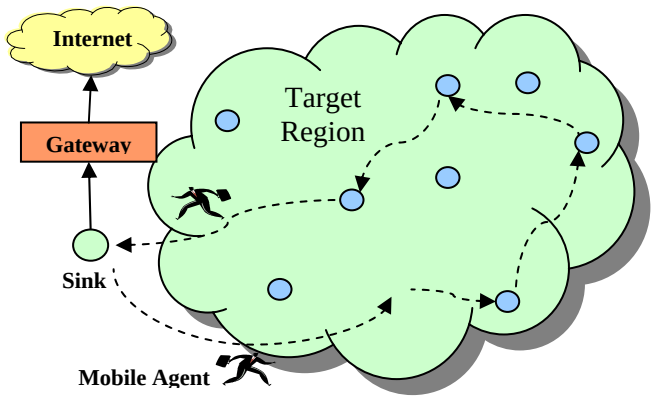


Figure 2. Mobile agent-based wireless sensor network

programming capability for cooperative data processing in WSNs [7].

MASPOT [8], MAPS [9][10] and MOBILE-C [11][12][13] are some of the studies regarding the integration of MAs in WSNs, but very few ones have been developed for Sun SPOT sensor devices [14]. They are compatible with Java 2 Micro Edition [15], and are supported by the Squawk Java Virtual Machine [16]. These studies are described in detail in related work section.

In this paper, it is aimed to give some insight on the issue of MA programming paradigm in WSNs and a **J**ava **A**gent-based **F**ramework for **S**un **SPOT**- JAFSPOT is proposed. This is a new agent-based framework programmable in Java for WSNs. It is based on Sun SPOT (Small Programmable Object Technology) sensor device technology that is an experimental platform for application programmers to develop WSN applications using Sun SPOT technologies. Because of their powerful structure, Sun SPOT sensor devices are widely used in the industry.

Agent-oriented programming of WSN applications are achieved in this framework using Java programming language. At the same time, event-based programming example is also used in the proposed framework. Therefore, all operations can be performed based on these events and the core components of the framework communicate through these events.

The remainder of the paper is organized as follows. MA systems recently developed for WSNs are investigated in Section 2. The proposed system architecture of the JAFSPOT framework and its main components are described in Section 3. In Section 4, a simple example is provided for exemplifying the MA-based application programming with JAFSPOT framework. Section 5 describes the testing and evaluation of proposed system. Finally, conclusion and the future work are mentioned.

II. RELATED WORK

Agent-based programming of WSNs is a very challenging issue because of the constrained resources of sensor devices. In addition, programming of WSNs is usually implemented as in an application specific manner and dependent on the application running in the system.

Some of the most popular MA-based WSN middleware systems proposed and implemented so far are described below.

MASPOT [8] is a MA-based system developed for Sun SPOT sensor devices. The authors claim that it is the only Java-based MA system for WSNs that currently provides code migration. Basic MA life cycles of creation, initialization, cloning and migration services are implemented in this framework. Its communication service provides primitives for agent-agent communications using tuple spaces and agents-base station communications using message passing. In addition, it only uses around 1.5% of the available flash memory and spends around 0.02% of the battery energy of sensor devices for moving an agent. It also extends the range of Java-based WSNs applications that can be built using current technology.

MAPS (Mobile Agent Platform for Sun SPOT) [9][10] is a MA-based platform for Sun SPOT sensor devices. It is established on the agent paradigm and provides the programming of WSN applications using Java language. The architecture of MAPS is component-based and presents the core services to agents. Event-based, state-based and agent-based approaches are combined in this platform. Since Squawk Virtual Machine operations are relatively slow, the time of MA migration is quite high. The serialization of agents into a message is a very time consuming operation. The radio stream communication between sensor devices is quite slow.

MOBILE-C [11][12][13] is an agent platform for mobile C/C++ agents. This platform is compatible with the IEEE the Foundation for Intelligent Physical Agents (FIPA) [17]. It extends FIPA standards to support MAs. It integrates an embeddable C/C++ interpreter into the platform as a MA execution engine and defines an agent mobility protocol to direct agent migration process. For agent migration, it uses FIPA agent communication language (ACL) messages encoded in XML. This offers a good solution for inter-platform agent migration in FIPA compliant agent systems. In this framework, scriptable C/C++ is chosen as a MA language. It is written in C with a small footprint, and it uses an embeddable C/C++ interpreter named Ch [18][19][20] to support the execution of MA C/C++ source code.

The system we described in this paper, JAFSPOT, differs from other systems in several ways. It is, to the best of our knowledge, one of the very few MA-based frameworks using Java programming language for WSNs that supports weak migration with isolate mechanism. In this mechanism, inner state and the private data of the MA residing on a sensor device can be saved in a format which the destination MA can handle. The agent code must be present on both sensor devices, so that any agent method can be created and initialized with the transferred agent state on the destination sensor device.

This isolate migration mechanism facilitates the mobility and extends the range of possible applications of Sun SPOT sensor devices. Furthermore, JAFSPOT provides event-based communication between MAs. Event-based approach is a useful abstraction in the context of WSNs. Particularly; occurrence of a physical event and the resulting reaction

 ISBN: 978-1-61208-231-8

according to this event provides a way to optimize the consumption of invaluable resources of resource-constrained WSNs.

III. SYSTEM ARCHITECTURE OF JAFSPOT FRAMEWORK

The block diagram of proposed system is depicted in Figure 3, and explained in detail below.

A. *Hardware*

Processor board, sensor board and battery are the three main components of Sun SPOT sensor devices. Interested readers may refer to [14] for detailed hardware components.

B. *SQUAWK Java Virtual Machine*

Squawk Java Virtual Machine is just over the hardware component. Here, fully capable J2ME CLDC 1.1 Java VM is supported by operating system. Hardware-independent and simultaneously working applications can be possible owing to the virtual machine.

Squawk JVM is realized for tiny devices with constrained capabilities using Java language and provides OS level mechanisms. It includes a mechanism for serializing the object graphs. All the pointers in a serialized object relocate in canonical addresses. This serialized form can be transformed into a new live object graph again.

Squawk JVM architecture is depicted in Figure 4. The most important characteristic feature of this architecture is a small and more remarkable compact byte code instruction set. Standard J2ME class files cover 35-45% less space compared with byte codes.

Isolate mechanism is one of the most important elements in the Squawk JVM architecture. Any application is represented as an object in this mechanism. More than one application can work in a single Squawk JVM. In this method, any application can conceptually run as fully isolated from other applications.

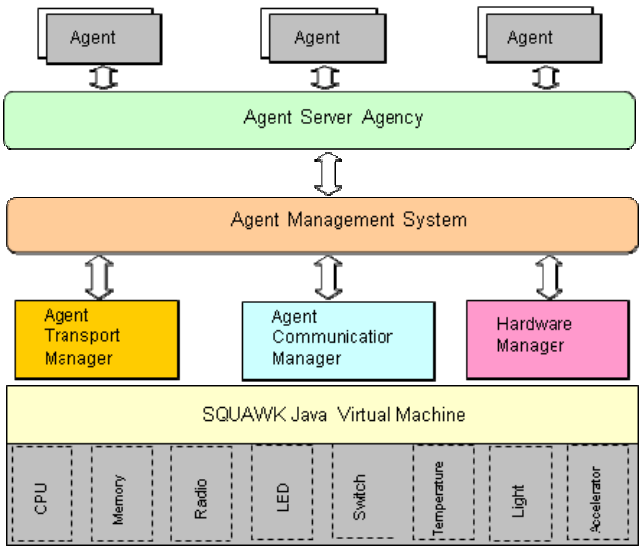


Figure 3. Block diagram of proposed system architecture

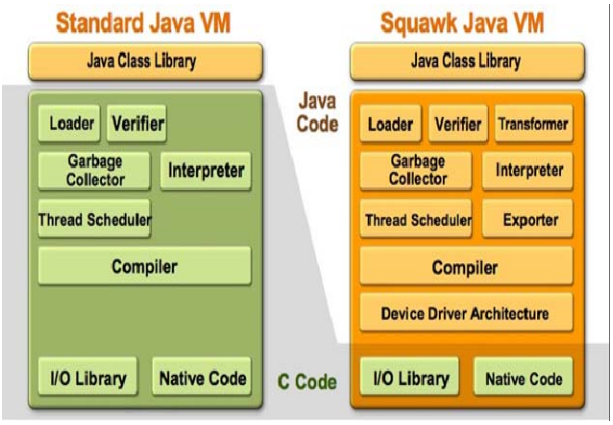


Figure 4. Squawk JVM architectural structure

It allows isolate migration which means that an isolate working in any instance of Squawk JVM to cease its operation, serialize into a file, send over network connection and work again in another instance of Squawk JVM.

1) *Isolate Mechanism*

While one application has multiple threads in standard Java ME applications, in practice only one application can work in standard Java VM at the same time. Nevertheless, Squawk JVM allows working of multiple applications on any Sun SPOT sensor device using a special class of Isolate. Thus, the operation of any application can be isolated from other applications. It prevents blocking the operation of one application from others. Each MIDlet-based application works in a separate isolate mechanism. All isolates can reach the resources of Sun SPOT hardware.

Isolate class provides a way to the instance of an isolate to work isolated from the instances of other isolates. Isolate mechanism is similar to the processes. Objects of any isolate are logically separated from objects of other isolates. Similarly, static variables of any isolate are logically separated from static variables of other isolates.

Isolate mechanism can be suspended in hibernation which stops working of both isolate and the threads of this isolate and can be serialized. The saved form of an isolate includes all the accessible objects, static variables and working contexts of all threads of this isolate. This saved form can be transferred to any file or other sensor devices over the sensor network. This saved isolate can be reopened, de-serialized and reactivated on the opposite side of the channel. An isolate can be in NEW, ALIVE, HIBERNATED and EXITED states.

C. *Agent Server Agency*

Agent Server Agency platform is located on the SQUAWK Java Virtual Machine component. This platform should be established on all Sun SPOT sensor devices and all components of the system work on this platform. This platform must be activated in the developed application in order to initialize the other components. New MAs that will work on the Sun SPOT sensor devices are to be added to the system with using this component. The 64-bit IEEE extended MAC address of the system running on the Sun SPOT sensor device is kept in this component.

 ISBN: 978-1-61208-231-8

D. Agent Management System

Agent Management System is the second component after the Agent Server Agency platform. This component operates as the brain of the system. It manages the events that happen throughout the system, connects and keeps the elements and provides the possibility of working together of the system components. This component makes connections with other components in order to perform the operations such as sending message, reading sensor values and synchronize timers performed by agents. This component is responsible for the required activities of agent creation, initialization, communication, migration, timing and termination. It provides the other components a way to work in a harmony.

E. Agent Transport Manager

Agent Transport Manager Component enables naming of agents, specifying the neighboring sensor nodes and neighboring agents dynamically and migration of agents from one sensor node to the other. In doing so, it provides a mechanism for serializing the agents into a message and migration of these agents to the neighboring sensor nodes. It also receives the messages containing the serialized agent coming from neighboring sensor nodes and opens and activates these agents with a reverse operation. This component is used for keeping the address and lists of the agents while migrating from a Sun SPOT sensor device to others within the communication range. It is also used for establishing a RadiostreamConnection between sensor devices before migrating of the agents to other sensor devices. Finally, it is used for receiving the agents sent from the other sensor devices.

F. Agent Communication Manager

Agent Communication Manager is the other component located on the Agent Server Agency platform. This component provides message-based asynchronous communication capability between agents working on the Sun SPOT devices. Thus, agents working on the different sensor devices can communicate with each other. Similarly, this component provides a way about communication of all the other components located on the Sun SPOT device. RadiogramConnection link can be established through the communication port between sender device and receiver device using this component. After the connection had been established, the Datagram was created for sending and receiving operations. In addition, all the events publish through this communication port to the neighboring sensor devices within the communication range.

G. Hardware Manager

The Hardware Manager component is located at the bottom of the Agent Server Agency platform. This component allows reading of data values from hardware resources like temperature sensor, light sensor, acceleration sensor, battery, switch and LED from Sun SPOT devices. Therefore, it can be possible to operate on the reading both sensor values and input/output values of hardware resources of Sun SPOT devices. It provides a way to perceive the physical temperature, light and three-dimensional acceleration as analog, to convert these analog values to numerical values and to evaluate these values as required.

IV. MOBILE AGENT APPLICATION

In this part of the paper, a MA application designed, developed and implemented using Java programming language. The purpose of this application is to demonstrate the rationale behind MAs working over the proposed system architecture on Sun SPOT devices. This MA-based application works on two real physical Sun SPOT devices. While the first one serves as the sender device, the second one serves as the receiver. In this application there are two MAs working on the sender device and one MA working on the receiver device. One of the sender side MAs is named MobileAgentSender and the other for MobileAgentMediator. MobileAgentMediator agent is migrated from sender device to the receiver device over wireless communication channel. MobileAgentReceiver agent works on the receiver device.

There are two different components of the proposed system, namely, the primary components and the secondary components. The primary ones are Agent Server Agency, Agent Management System, Agent Transport Manager, Agent Communication Manager and Hardware Manager. The secondary ones are Light Sensor, Temperature Sensor, Accelerometer Sensor, LED and Switch. All these components on the two Sun SPOT devices should be activated and worked in order to MAs to work. After all the components had been activated on the two Sun SPOT devices, the MAs added to the system.

A. MobileAgentSender

There are six conditions for MobileAgentSender agent working on sender Sun SPOT device in this application. These conditions are Begin State, Wait_Message State, Event_Creation State, Capture_Value State, Transmit_Value State and End State. These conditions are illustrated in Figure 5.

```
BEGIN:
    AGENT_START:
        Create LED_ON/LED_OFF events used for producing a binary count up
        to 256 on the 8 tri-color LEDs on Sun SPOT sensor device in red color
WAIT_MESSAGE:
    MESSAGE:
        Create LED_FLASH event used for flashing all the 8 tri-color LEDs ten
        times in blue color
        Create SWITCH_ON event
EVENT_CREATION:
        Create TEMPERATURE, LIGHT, ACCELERATION, BATTERY event
CAPTURE_VALUE:
    TEMPERATURE, LIGHT, ACCELERATION and BATTERY:
        Add light, temperature, acceleration and battery values to related variable
    SWITCH_ON:
        Create MobileAgentMediator agent
        Create LED_FLASH event used for flashing the first LED of 8 tri-color
        LEDs in red color
TRANSMIT_VALUE:
        Create related event for MobileAgentMediator agent to be sent
        Piggy-back the data to the MobileAgentMediator agent as a payload
END:
        Stop agent operation
```

Figure 5. States/actions of MobileAgentSender agent

B. *MobileAgentReceiver*

There are four conditions for MobileAgentReceiver agent working on the receiver side Sun SPOT sensor device in this application, including Begin State, Switch_On State, Circulated_Data State and End State. These conditions are illustrated in Figure 6.

```
BEGIN:
    AGENT_START:
        Create LED_ON/LED_OFF events used for producing a binary count up to
        256 on the 8 tri-color LEDs on Sun SPOT sensor device in red color
        Create SWITCH_ON event
SWITCH_ON:
        Discover the other mobile agents
        Create and send message event
CIRCULATED_DATA:
    MESSAGE:
        Fragment obtained data into meaningful parts using StringTokenizer
        Print out light, temperature, acceleration and battery values on the screen
END:
        Stop agent operation
```

Figure 6. States/actions of MobileAgentReceiver agent

C. *MobileAgentMediator*

There are three conditions for MobileAgentMediator agent working on the sender side device and will migrate to the receiver side in this application. These conditions are Begin State, Migration State and End State. These conditions are illustrated in Figure 7.

```
BEGIN:
    AGENT_START:
        Obtain the value of data from related variable
        Discover the other neighboring mobile agents
        Declare its migration request to these identified sensor devices
MIGRATION:
        Migrate to these identified sensor device
END:
        Stop agent operation
```

Figure 7. States/actions of MobileAgentMediator agent

V. TEST AND EVALUATION

This section describes the testing and evaluation of proposed system explained in Section IV. The purpose of this test scenario is to demonstrate the rationale behind MAs working over the proposed system architecture on Sun SPOT Java Development Kit with Sun SPOT SDK v5.0 (Red). This kit includes a base station and two Sun SPOT sensor devices equipped with sensor boards and rechargeable batteries. This application is developed using the Apache Ant Server, Java Development Kit 1.6.0_31 and NetBeans IDE 7.1.1 Integrated Development Environment.

Since the amount of energy spent by sender and receiver side agents is a critical issue for WSNs we evaluated this parameter. Here, we tested five issues namely, battery current drawn while the MA migration, available capacity, MA creation time, MA migration time and MA termination time. We repeated and obtained 15 different values for this test.

There are three key points for testing the migration cost of MA. The first point is where the MA residing on the sender side sensor node asks for the migration. The second point is where the sender side MA received an ACK used for acceptance of migration from receiver side sensor node. The third point is where the sender side MA successfully migrates to the destination side node. At these points, we captured the maximum battery current drawn from sender and receiver side nodes. These experiment values are depicted in Figure 8.

Here, we compare our results with the values of Table 1 in related research paper on MASPOT [8]. As it can be seen from these results, the mean spent energy of JAFSPOT was 0.71559986 milliampere for the sender side and 0.453732553 milliampere for the receiver side. Here this gives an overall mean of 0.584666207 milliampere. Similarly, mean spent energy of MASPOT [8] was 0.1577 milliampere for the sender side and 0.1257 milliampere for the receiver side, giving an overall mean of 0.1417 milliampere.

We have also studied the available capacity of the sender and receiver side sensor nodes. Each Sun SPOT sensor node is equipped with a 3.7 V rechargeable 770 milliAmperehour Lithium-Ion battery. The obtained values are depicted in Figure 9. Here, the mean percentage of battery use is on average 0.099388869% for the sender side and 0.06301841% for the receiver side battery capacities. Considering these average values obtained with these tests, sender side sensor node spent around 57.71% more energy than the receiver side sensor node.

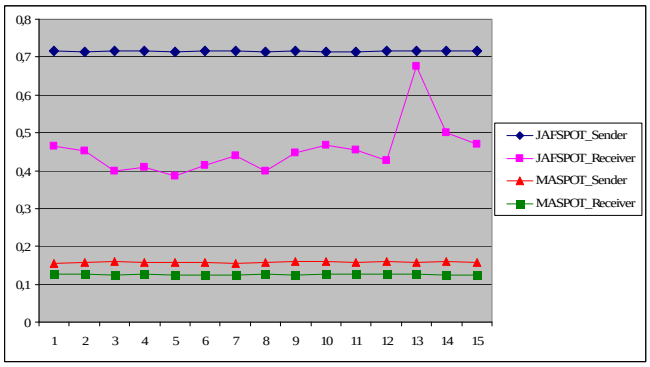


Figure 8. Agent Migration Cost in milliampere

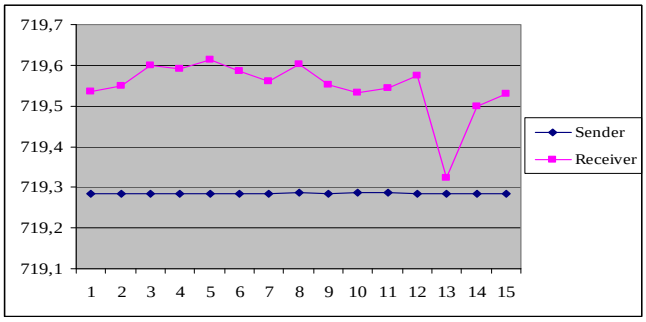


Figure 9. Available Capacity

 ISBN: 978-1-61208-231-8

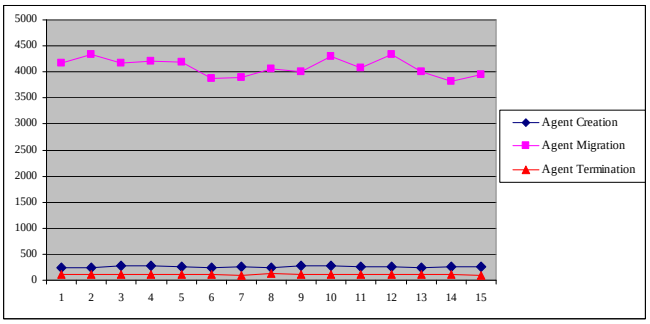


Figure 10. Elapsed time in milliseconds

We have also tested the MA creation time, migration time and termination time for the evaluation of cost of these parameters. The results are shown in Figure 10. It can be seen that, the mean agent creation time was 259.2666667 milliseconds. Similarly, the mean agent migration time and agent termination time were 4093.4 milliseconds and 108.9333333 milliseconds, respectively. Considering these values, agent migration time is much greater than the agent creation time and agent termination time. Because the operations of Squawk JVM are relatively slow, the serialization of agents into a message is a very time consuming process, and the radio stream communication between sensor devices is quite slow.

VI. CONCLUSION

The design, development, deployment and implementation of a Java Agent-based Framework for Sun SPOT- JAFSPOT, has been presented in this article. To the best of our knowledge, JAFSPOT is one of the very few Java-based, MA-based and event-based systems for Sun SPOT sensor devices of WSN that supports isolate migration. With this framework, it is possible to specify real world scenarios using static and/or MA-based applications. It also facilitates the programming of event-based and agent-based applications. Event-based approach is a particularly useful abstraction in the context of WSNs. Particularly; this approach provides a way to optimize the consumption of invaluable resources of resource-constrained WSNs. It exemplifies how to program different dynamic behaviors of the MAs during their lifetime. Providing weak migration of isolate mechanism is an important facility when considering usage of MAs to support WSN reprogramming. The possibility of executing MAs on Sun SPOT sensor devices extends considerably the varieties of applications for this platform.

Our ongoing efforts have been devoted to extending this framework for a real world application and adding a security aspect.

REFERENCES

[1] I. F. Akyildiz, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks”, IEEE Communications Magazine, vol. 40 (8), pp. 104-112, 2002.

[2] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey”, Computer Networks, vol. 52 (12), pp. 2292-2330, 2008.

[3] F. Aiello, G. Fortino, R. Gravina, and A. Guerrieri, “A Java-based platform for programming wireless sensor networks”, The Computer Journal, vol. 54 (3), pp. 439-454, 2010.

[4] S. González-Valenzuela, M. Chen, and V. C. M. Leung, “Applications of mobile agents in wireless networks and mobile computing”, Advances in Computers, Marv Zelkowitz (Ed.), vol. 82, pp. 113-163, 2011.

[5] M. Chen, T. Kwon, and Y. Choi, “Mobile agent-based Directed Diffusion in wireless sensor networks”, EURASIP Journal on Applied Signal Processing, (1), 2007.

[6] E. Shakshuki, H. Ghenniwa and M. Kamel, “Agent-base system architecture for dynamic and open environments”, Journal of Information Technology and Decision Making, vol. 2 (1), pp. 105-133, 2003.

[7] P. Wang, “A brief survey on cooperation in multi-agent system”, International Conference on Computer Design and Applications (ICCDA), vol.2, pp. 39-43, 25-27 June 2010.

[8] R. Lopes, F. Assis, and C. Montez, “MASPOT: A mobile agent system for Sun SPOT”, Tenth International Symposium on Autonomous Decentralized Systems, Tokyo, 2011.

[9] F. Aiello, G. Fortino, R. Gravina, and A. Guerrieri, “MAPS: A mobile agent platform for Java Sun SPOTs”, Proc. 3rd Int. Workshop on Agent Technology for Sensor Networks (ATSN), Budapest, Hungary, 12 May 2009.

[10] F. Aiello, G. Fortino, R. Gravina, and A. Guerrieri, “A Java-based agent platform for programming wireless sensor networks”, The Computer Journal, vol. 54 (3), pp. 439-454, 2010.

[11] B. Chen, H. H. Cheng, and J. Palen, “Mobile-C: a mobile agent platform for mobile C/C++ agents”, Software: Practice. and Experience, vol. 36, pp. 1711-1733, 2006.

[12] B. Chen and H. H. Cheng, “A runtime support environment for mobile agents”, Proceedings of the 2005 ASME/IEEE International Conference on Mechatronic and Embedded Systems and Applications (MESA05), Long Beach, CA, September 2005. American Society of Mechanical Engineers: New York, pp. 37-46, 2005.

[13] B. Chen, “Runtime support for code mobility in distributed systems”, PhD Thesis, Department of Mechanical and Aeronautical Engineering, University of California, 2005.

[14] Sun™ Small programmable object technology (Sun SPOT). (2012), http://www.sunspotworld.com/.

[15] Sun Microsystems. Java 2 Platform, Micro Edition (J2ME)-Connected Limited Device Configuration-Specification-version 1.1, Mar. 2003.

[16] D. Simon and C. Cifuentes, “The Squawk Java Virtual Machine: Java on the Bare Metal”, Proc. 20th Object-Oriented Programming, Systems, Languages and Applications (OOPSLA 2005), San Diego, CA, USA, October 16-20, pp. 150-151.ACM, NewYork, NY, USA, 2005.

[17] IEEE Foundation for Intelligent Physical Agents (FIPA). Agent Communication Language Specifications. (2012), http://www.fipa.org/repository/aclspecs.html.

[18] H. H. Cheng, “Scientific computing in the Ch programming language”, Scientific Programming, vol.2 (3), pp. 49-75,1993.

[19] H. H. Cheng, “Ch: A C/C++ interpreter for script computing”, C/C++ User’s Journal, vol. 24 (1), pp. 6-12, 2006.

[20] Softintegration, Inc. “Ch: An Embeddable C/C++ Interpreter”, (2012), http://www.softintegration.com.

 ISBN: 978-1-61208-231-8

Finding Diverse Shortest Paths for the Routing Task in Wireless Sensor Networks

Wilton Henao-Mazo and Ángel Bravo-Santos
Departamento de Teoría de la Señal y Comunicaciones
Universidad Carlos III de Madrid
Avda. de la Universidad 30, Leganés, 28911 Madrid, Spain
{*wiltonhm, abravo*}*@tsc.uc3m.es*

***Abstract*—Wireless Sensor Networks are deployed with the idea of collecting field information of different variables like temperature, position, humidity, etc., from several resource-constrained sensor nodes, and then relay those data to a sink node or base station. Therefore, the path finding for routing must be carried out with strategies that make it possible to manage efficiently the network limited resources, whilst at the same time the network throughput is kept within appreciable levels. Many routing schemes search for one path, with low power dissipation that may not be convenient to increase the network lifetime and long-term connectivity. In an attempt to overcome such eventualities, we proposed a scenario for relaying that uses multiple diverse paths obtained considering the links among network nodes, that could provide reliable data transmission. When data is transmitted across various diverse paths in the network that offer low retransmission rates, the battery demand can be decreased and network lifetime is extended. We show, by using simulations, that the reliability in packets reception and the power dissipation that our scheme offers compare favourably with similar literature implementations.**

***Keywords*-WSNs; Wireless Sensor Networks; K Shortest Paths; Diverse Paths.**

I. INTRODUCTION

Wireless Sensor Networks (WSN) have been one of the trending research topics for several years due to their particular features among which are worth to highlight topologies flexibility, distributed detection capacity, low energy consumption and stand alone operation. All these WSN features allow to cope different tasks such as target tracking for mobile agents, event detection, environment information gathering and remote monitoring/controlling. At the same time this technology must perform the activities they are required to accomplish, bearing in mind that there are some limitations like the energy source that in almost all the cases is a battery, the low processing capacity, the unpredictable reliability on the information delivery due to some phenomena of wireless channel, the relative-low transmission rates and the short range in wireless communication.

In a WSN, there exists a task which consists in taking the data through the network from one node to another in a determined period of time, and it is known as the relaying or the forwarding of data packets. In this process, an important issue necessary to deal with is the transmission reliability, whilst energy efficiency is maintained in order to guarantee a considerable network lifetime. These issues have been treated in routing tasks and mechanisms implemented in the application layer related to energy saving goal [1][2][3]. One justification to pay attention in obtaining quite good reliability levels in communication is the belief that significant energy resources can be saved when the number of required retransmissions is reduced [4]. On the other side some, of the referenced works only try to obtain a single optimum route by which the data traffic mainly flows from source node to destination node, and such strategy can incur faster energy depletion of the nodes of this route. Finding multiple paths, obtained based on the Ad hoc On-Demand Distance Vector (AODV) that requires distances and hop count, can be used for the relaying task and it seems to be a good option when network survivability is required [2]. In the present paper, a different strategy is implemented. Here, the idea of finding multiple paths which have certain degree of diversity among them becomes important. In this way, it is possible to guarantee reliable successfully transmitted data rates and the power dissipation is distributed among the nodes involved in the data forwarding task.

As seen before, one important aspect in routing is finding multiple paths. Hence, it is important to know that the K shortest paths problem is a natural and widely-studied generalization of the shortest path problem in which not one, but several paths in increasing order of length are sought. The K shortest paths problem in which paths can contain loops turns out to be significantly easier. But the problem of determining the K shortest loopless paths has proved to be more challenging. The problem was first examined by Hoffman and Pavley [5]. For undirected graphs, the most efficient algorithm, proposed by Katoh et al. [6], has the complexity of $O(K(|L| + |M|\log|M|))$ ($|L|$ the number of edges and $|M|$ the number of nodes). For the most general case, the best known algorithm is that proposed by Yen in [10]. This algorithm has achieved the complexity of $O(K|M|(|L| + |M|\log|M|))$. Here, we use the Yen's algorithm as a basis for our proposal.

The organization of the paper follows with a brief outline of Yen's algorithm in Section II, jointly with some useful assumptions and graph theoretic concepts. Later, in Section III, the proposed algorithm to find diverse shortest paths (DSP) in a WSN is presented. Section IV shows simulation

 ISBN: 978-1-61208-231-8

results and an analysis about the proposed scheme, and finally, some conclusion of the developed work are drawn in Section V.

II. PRELIMINARIES

In order to define in a clear way what is wanted to do in a WSN, we are using classical statements from graph theory by which our wireless network of sensors can be represented as a pair $G = (M, L)$. Here, G represents an undirected graph where M is the set of m sensor nodes, each of them identified by a unique mote number inside the net, and L is the set of possible wireless links between nodes $i \in M$ and $j \in M$. For simplicity, it is necessary to consider a cost communication matrix $A^{m \times m}$, in which each consigned entry $a_{ij} \in \{\mathbb{R}^+ \cup +\infty\}$ holds for the cost or weight that is required to establish the links of the previously described set L.

A. Some network assumptions

- Node's mobility in the network is not allowed, hence every node has a fixed position.
- Ordinary sensor nodes have the same capabilities, the same radio-transmitter devices and constrained power resources.
- The sink node is assumed to have unconstrained resources.
- Symmetric cost model is assumed. This means link cost of transmit data from sensor i to sensor j is the same than in the opposite direction.
- The received signal strength (RSS) can be measured in each of the nodes, without significant cost in power consumption.
- Without loss of generality, a log-normal path loss radio propagation model is assumed as a well-suited approximation for the link layer modelling of a wireless sensor network. Such a model is deeply described in [7] [8].
- In order to guarantee a good performance of the network with respect to communication reliability, an ACK mechanism is used in each hop of the transmission rather than an end-to-end error recovery strategy.

B. An algorithm that finds shortest paths

One of the most important algorithms developed for finding certain amount of paths between a pair of source-destination nodes in a graph is the Yen's algorithm (1971) [10]. This is based on a deviation principle. First, let us denote the source node by $s \in M$ from which it is desired to get the sink node $t \in M$, through K shortest loop-less paths. These paths form a set of K components, $P = \{P_1, P_2, \cdots, P_K\}$. At the same time, each path of the latter set is defined by the sequence $P_K = \langle s = v_1^K, v_2^K, \cdots, v_i^K = t \rangle$, where v_i^K is the i-*th* node of the K-*th* shortest path. In the next algorithm, there is a brief outline of this procedure.

Algorithm 1 Yen's algorithm

Require: A, s, t, K.

1: $P^1 \leftarrow$ Dijkstra(s, t)
2: $D \leftarrow \{P^1\}$ %Set of candidates
3: $P \leftarrow \{\}$ %Set of the K shortest paths
4: **for** k from 2 to K **do**
5: $SP \leftarrow$ the shortest path in D
6: $v \leftarrow$ the deviation node (SP, P)
7: $P \leftarrow P + SP$
8: **while** $v \neq t$ **do**
9: discard all nodes of SP from s to v
10: discard each output link of v which belongs to P
11: $SP' \leftarrow$ Dijkstra(v, t)
12: join SP' and SP from s to t
13: $D \leftarrow D + \{SP'\}$
14: restore all discarded nodes and links
15: $v \leftarrow$ successor(v, SP)
16: **end while**
17: **end for**

As it can be figured out from Algorithm 1, given an adjacency matrix and a source-sink pair of nodes, the algorithm is initiated by calculating the shortest path P^1 (line 1) and initializing some variables. Then the algorithm will perform K iterations. At the k-*th* iteration, the algorithm extracts the shortest path stored in candidates set D. This path is the K-*th* resulting path from s to t. Then, the deviation node is calculated from all the $K - 1$ paths in SP. To avoid recalculation of the already computed paths, the algorithm discards certain nodes and links as it is shown in lines 9 and 10. The shortest path SP' between deviation and source node is calculated with the remaining graph. Then, SP' joins the sub-path of the K-*th* shortest path from source to deviation node and saves this new produced path in the candidate set D. Finally, all the links and nodes previously discarded are restored and the algorithm moves to the successor of the deviation node (line 15) in the K-*th* shortest path.

III. PROPOSED ALGORITHM

As previously noted, algorithms that find shortest paths need metric information. This metric information can be considered as the cost of possible inter-node links, and according to this the algorithms try to minimize the total cost of paths. As mentioned before, the packet reception rate (PRR) will be useful for finding reliable paths by which data is relayed from source to destination nodes. Trying to avoid significant delays in the process of path discovery, the PRR can be computed easily at each node by the following procedure: since each sensor node is able to obtain the

 ISBN: 978-1-61208-231-8

RSS when an incoming message is correctly received, based on this measure, the wanted metric can be estimated. In order to illustrate how to estimate the PRR when there exists a BPSK modulation, with a measurement of RSS and a good estimated characterization of noise, the SNR can be computed as $\gamma[dB] = RSS - P_n$. Then, a bit error probability is calculated for the current case as [7]

$$P_e = \mathcal{Q}(\sqrt{2\gamma \frac{B_n}{R}}), \quad (1)$$

where B_n is the noise bandwidth and R is the bit data rate. Furthermore, provided that all bits are received without errors, there exists a correct reception. Then, we can derive the probability of successfully packet reception for a frame of f-bytes length at certain distance as[7]

$$p = (1 - P_e)^{8f}. \quad (2)$$

Finally, the PRR can be calculated regarding a NRZ encoding mechanism with preamble length L [7] with the expression[7]

$$PRR = (1 - Pe)^{8L}(1 - Pe)^{8(f-L)}. \quad (3)$$

So far, the computation of the PRR has been described, but the useful metric for our algorithm is missing. If we pretend to use an algorithm that yields shortest paths, the raw obtained PRR is non meaningful for our desired goals of power efficiency through reliable data relaying. Thus, each possible communication link is going to have the inverse of the PRR as metric, or cost, between nodes i and j for finding the shortest paths,

$$LC(i,j) = 1/PRR_{ij}. \quad (4)$$

These link costs are consigned in the previously defined network cost communication matrix. A total link cost (TLC) of such paths are computed within the Yen's algorithm as

$$TLC_{P_{st}} = \sum_{(i,j)\ links\ \in\ P_{st}} LC(i,j). \quad (5)$$

Diverse paths from K shortest path

Given the Yen's algorithm as the basis for what is wanted to achieve, when this algorithm returns K paths, they usually have many links in common. But we do not really need too much redundancy in the routes avoiding this way the faster energy depletion of the nodes involved. This kind of "trouble" can be explained by the principle of deviation nodes. However, in the present work a filtering or selection applied over the set of K shortest paths is introduced. With this selection certain degree of diversity can be achieved. It is suspected that transmitting data packets in a WSN over diverse paths lead us to trustful communication levels by avoiding the amount of retransmissions that might appear in a single path case. Algorithm 2, shown below, outlines how to proceed to obtain paths as diverse as possible starting from the K shortest paths,

Algorithm 2 Diverse paths selection

Require: A, s, t, K, α.

1: $IncludedLinks \leftarrow \{\}$ % Set of appearing links
2: $w_{P_K} \leftarrow 0$ % Array of K weights of paths
3: Get $P_1, P_2, \cdots P_K$ the K shortest paths by Yen's algorithm between s and t.
4: $IncludedLinks \leftarrow$ All $(i,j) \in P_1$
5: $w_{P_1} \leftarrow 1$
6: **for** k from 2 to K **do**
7: $\quad w_{P_k} \leftarrow \sum_{(i,j)\in P_k} \frac{LC(i,j)}{TLC(i,j)} G(i,j)$
8: $\quad$ **for** each link $(i,j) \in P_k$ **do**
9: $\quad\quad$ **if** $(i,j) \notin IncludedLinks$ **then**
10: $\quad\quad\quad IncludedLinks \leftarrow IncludedLinks + (i,j)$
11: $\quad\quad$ **end if**
12: $\quad$ **end for**
13: **end for**
14: $DSP \leftarrow P_k$ whose $w_{P_K} \geq \alpha$

The procedure showed in Algorithm 2 is conceived on the idea of selecting diverse paths. After coming up with K shortest paths by using Yen's algorithm, we proceed to fill in the set $IncludedLinks$. This set contains links from the K shortest paths such that if we analysed these paths in ascendant order, the links that appear for the first time (hence, they have not been in this set before) in the search would be in the $IncludedLinks$ set. In the Algorithm 2 can be noted how all the links of the shortest path 1 are in the $IncludedLinks$ set.

The weight of each one of the K paths is computed in the present work as,

$$w_{P_k} = \sum_{(i,j)\in P_k} \frac{LC(i,j)}{TLC_{P_k}} G(i,j), \quad (6)$$

which, at the same time, is depending on $G(i,j)$, a general function which indicates the previous inclusion of the link into a previous path and defined as,

$$G(i,j) = \begin{cases} 1 \text{ if } (i,j) \notin IncludedLinks \\ 0 \text{ if } (i,j) \in IncludedLinks. \end{cases} \quad (7)$$

The computation carried out in line 1 of Algorithm 2 is laying out how dissimilar the paths are, in the sense of the amount of links they differ, and is giving a weight or importance to the path depending on individual link costs, as well. Finally, another important aspect to review in the latter algorithm is the threshold α. From the different K paths we are selecting a reduced number of them if and only if their weights fulfil the condition $w_{P_K} \geq \alpha$. Such threshold is an arbitrary fixed value within the range $0 \leq \alpha \leq 1$, so the greater the threshold the fewer number of links the selected routes share.

In the example shown in Figure 1, where is depicted in first place (sub-figure (a) above) the resulting $K = 20$

 ISBN: 978-1-61208-231-8

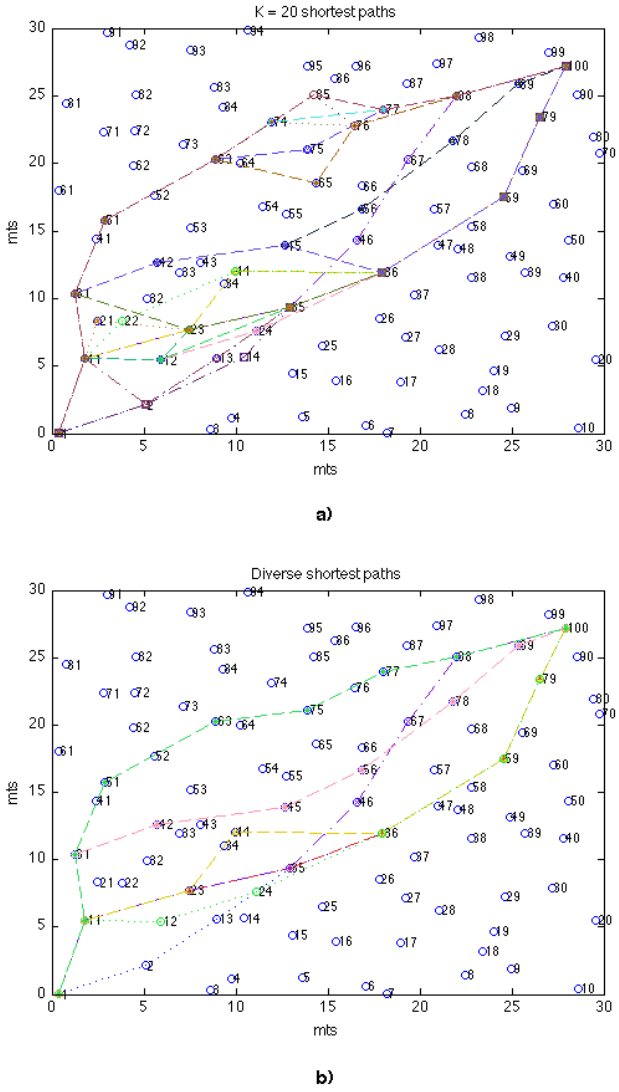


Figure 1. Obtained shortest paths example in a WSN.

shortest paths in a WSN, and in other (sub-figure (b) below) the shortest paths selected from the previous ones by the Algorithm 2 with $\alpha = 0.35$. As can be verified here, whilst Yen's algorithm returns certain routes that seem to be copies from a previous one except by couple of links. With the diverse paths selection carried out over that set, we keep paths with relative few redundant links.

IV. Simulations and Performance Analysis

We wrote the code of a customized discrete time, event-driven wireless sensor network simulator in MATLAB in order to evaluate the efficiency of the algorithm in a packet level environment. For simplicity on simulating the net, a simple CSMA/CA mechanism is used in MAC layer to avoid signal conflicts. Also the physical link layer model values reported in [7][8][9] are used. Detailed fixed simulation parameters are shown briefly in Table I.

Table I
Parameter values used in simulation

Parameter	Value
Network topology	randomly uniform
Network area	$30 \times 30\ m^2$
Data rate	19.2 Kbps
Tx Power	-7 dBm
Carrier frequency	900 MHz
Path loss exponent, n	4.7
Shadowing standard deviation, σ_n	3.2
Modulation	BPSK
Noise bandwidth, B_n	30 KHz
Noise floor	-105 dBm
Encoding	NRZ
Frame size, f	50 bytes
Preamble length, L	2 bytes

We compare our proposed diverse shortest paths (denoted by DSP) algorithm with a rough implementation of the algorithm EDA proposed in [11], that finds multiple disjoint paths based on minimum spanning trees rooted at both source node and destination node, coming up with multiple paths for packet forwarding. Such EDA implementation is rough, due to it is made simulating its distributed nature by using a heap, where events with a time stamp are managed through this data structures. A second comparison is carried out with a Naive algorithm that finds disjoint paths by the following procedure: find the shortest path between source and sink nodes, then remove the nodes in the first obtained shortest path from the network; find another shortest source to sink path in the remaining network and delete them once obtained. Iterate this way until a previously defined number of paths has been found. Both algorithms used for comparison, made use of the metric LC presented in Section III , as well as our DSP proposed algorithm.

The performance of our algorithm is demonstrated by simulating a data packet forwarding environment between a source node and a sink node. Then, we measure the rate of successfully delivered packets when a source node generates 10000 information packets. Such rate is taken as the ratio of packets that reached the destination nodes between the total number of packets generated in the source. Every packet has a number of packet which helps to know whether packet loss given a period of time occur. For all the algorithms, we vary the network nodes density (# of nodes/m^2) by increasing the number of nodes from 50 to 300 and keeping the area where the net is deployed as specified in Table I.

Simulations results are contained in Figure 2. Taking

 ISBN: 978-1-61208-231-8

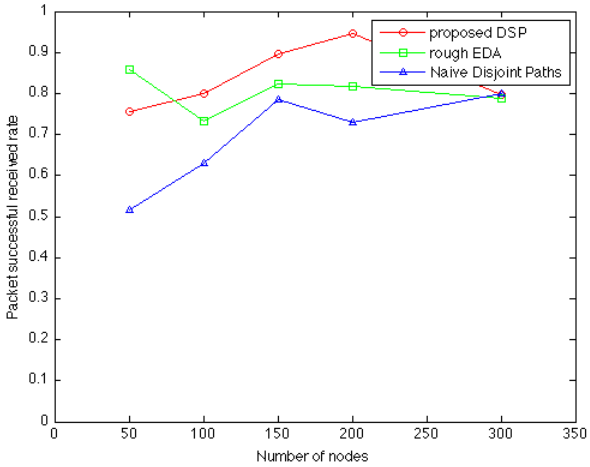


Figure 2. Reliability in packet reception varying nodes in the WSN.

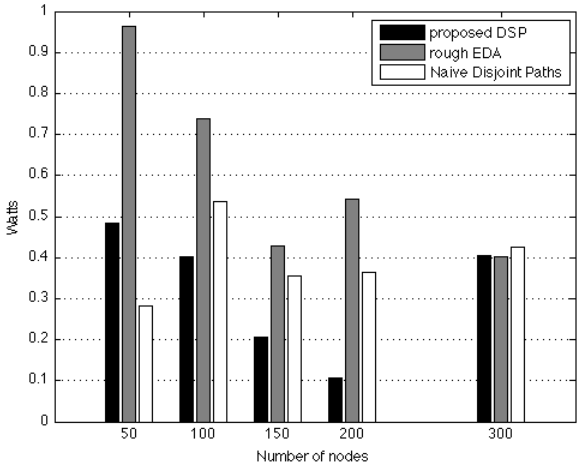


Figure 3. Average power dissipated in retransmissions.

into account that the number of nodes in the network has been varied and the transmission of the packets has been simulated for the 3 algorithms previously commented; it is remarkable how in almost all the cases our DSP proposed algorithm has the best performance among these 3 algorithms. The Naive disjoint paths algorithm has generally the weakest successful reception rate because it attempts to look for paths in a greedy way and ignoring the possibility of finding multiple paths at each iteration. All the three algorithms seem to converge to a slightly good reliability level of about 0.80 when the WSN node density is increased.

An additional important aspect that can be obtained from simulation results is the average power required in retransmitting when packet loss occurs. In Figure 3, we present the power dissipated in retransmission of the three commented strategies. Our proposal has neat advantage when the number of nodes is 200. The DSP algorithm is wasting only about 19% and 29% from the power required by the Naive algorithm and the rough version of EDA, respectively.

V. Conclusion and Future Work

To obtain diverse paths for the routing task in the WSN, we proposed an algorithm that has as a main core Yen's algorithm, an efficient algorithm for computing the K shortest path problem. Here we compare our proposed algorithm with one that finds multiple disjoint paths based on a spanning tree construction [11] trying to look for some advantage, and with a Naive procedure that finds multiple node-disjoint paths. Our proposal presents some advantages over the other two algorithm used for comparison. Simulations show that relaying through the routes our proposed algorithm finds, reliable communication levels are obtained, while considerable energy saving takes place in the network. This is because of the reduction on retransmission events by selecting reliable paths. Another reason is that the network lifetime is increased due to a distributed usage of the network. A distributed usage can be seen when different nodes which compose the diverse shortest paths are used each time.

Another observation obtained from the results is the unpredictable behaviour that all the finding paths algorithms present with the variation of the number of nodes or network density. In this work for example, the throughput curves of the three algorithms do not follow similar patterns. Hence, this might be a possible improvement aspect which needs to be worked on further. Besides, a very interesting future line work is an implementation of Yen's algorithm that could take advantage of the distributed processing power present in WSNs.

Acknowledgment

This work has been partially supported by the Spanish government (Ministerio de Educación y Ciencia 2009-14504-C02-01, Consolider-Ingenio 2010 CSD2008-00010).

References

[1] M.J. Baek, K.I. Kim and S.H. Cho , "*A revised Mint-Route protocol in wireless sensor networks*". Information and Communication Technology Convergence (ICTC), 2010 International Conference on , no., pp. 258-259, 17-19 Nov. 2010

[2] P. Hurni and T. Braun, "*Energy-Efficient Multi-Path Routing in Wireless Sensor Networks*". In Proceedings of the 7th International Conference on Ad-Hoc, Mobile and Wireless Networks (ADHOC-NOW 08), Sophia Antipolis, France, 1013 September 2008, pp. 7285.

[3] R. Vidhyapriya and P.T. Vanathi,"*Energy Aware Routing for Wireless Sensor Networks*". Signal Processing, Communications and Networking, 2007. ICSCN '07. International Conference on, pp. 545-550, 22-24 Feb. 2007.

 ISBN: 978-1-61208-231-8

[4] J. Zuo, C. Dong, S. Ng, Y. Lie-Liang and L. Hanzo, "*Energy-Efficient Routing in Ad Hoc Networks Relying on Channel State Information and Limited MAC Retransmissions*". In VTC2011-Fall, San Francisco, United States, 05 - 08 Sep 2011.

[5] W. Hoffman and R. Pavley,"*A method for the solution of the Nth best path problem*". Journal of the ACM, 6: pp. 506-514, 1959.

[6] N. Katoh, T. Ibaraki and H. Mine,"*An efficient algorithm for k simple paths*". Networks, 12: pp. 411-427, 1982.

[7] M. Zuniga and B. Krishnamachari,"*Analyzing the transitional region in low power wireless links*". IEEE SECON, Santa Clara, CA, October 2004.

[8] M. Zuniga and B. Krishnamachari,"*Link layer models for wireless sensor networks*". USC, Dec. 2005, unpublised.

[9] K. Sohrabi, B. Manriquez and G. Pottie,"*Near ground wide-band channel measurement in 800-1000 MHz*". Proceeding of IEEE VTC, Sep. 1999.

[10] J. Y. Yen,"*Finding the K shortest loopless paths in a network*". Management Science, Vol. 17, pp. 712-716, 1971.

[11] K. Zhang and H. Gao,"*Finding multiple length-bounded disjoint paths in wireless sensor networks*". Wireless sensor networks, Vol. 3, pp. 384-390, 2011.

 ISBN: 978-1-61208-231-8

Potential-Based Downstream Routing for Wireless Sensor Networks

Shinya Toyonaga*, Daichi Kominami*, Masashi Sugano† and Masayuki Murata*
*Graduate School of Information Science and Technology, Osaka University, Osaka, Japan
Email:{s-toyonaga, d-kominami, murata}@ist.osaka-u.ac.jp
†School of Knowledge and Information Systems, College of Sustainable System Sciences,
Osaka Prefecture University, Osaka, Japan
Email:sugano@kis.osakafu-u.ac.jp

***Abstract*—In wireless sensor networks designed for periodic monitoring, various many-to-one upstream (sensor-to-sink) routing protocols have been studied. Potential-based routing (PBR) is one such protocol, and can achieve low overhead, high scalability, and efficient load balancing. However, in PBR, unicast messages such as special instructions from a sink node to a certain node are not taken into consideration. In this paper, we propose a potential-based downstream routing protocol (PBDR), in which each sink node constructs an independent potential field and all sensor nodes and sink nodes have a set of potentials determined on each potential field. We refer to the set of potentials as virtual coordinates, based on which we define virtual distance. When a node with downstream data decides a next hop, it calculates the virtual distances from neighbor nodes to the destination node, and forwards the data to the neighbor node closest to the destination node. Through simulation experiments, we show that, given a suitable node density, PBDR attains a data delivery ratio greater than 99.5%. We also show that the data delivery ratio recovers immediately after the failure of 30% of sensor nodes or the failure of a sink node.**

Keywords*-*sensor networks; potential-based routing; downstream routing; simulation.

I. INTRODUCTION

In wireless sensor networks designed for periodic monitoring, various many-to-one upstream (sensor-to-sink) routing protocols have been studied. In some applications, specific requirements must be met for downstream (sink-to-sensor) data delivery. For example, a sink node sends a query to a specific sensor node upon receiving abnormal data from it, or a sink node sends a message in order to change the frequency of sensing in a specific domain.

Many potential-based routing protocols have been proposed for upstream (sensor-to-sink) data transmission [1-3]. These potential-based upstream routing protocols (PBUR) aim for low overhead, high scalability, and energy balancing. In PBUR, all nodes have a potential. Each node calculates its potential based on local information, such as their neighbor nodes' potentials or residual energy, and a sensor node whose hop count to a sink is smaller (larger) has a higher (lower) potential. Therefore if a node sends data to its neighbor node with higher potential, the data will ultimately reach a sink node. Since these potential fields are constructed on the basis of purely local information, PBUR is scalable. Moreover, if these potential fields are constructed based on residual energy, load balancing can be realized. However, in these protocols, the delivery of downstream (sink-to-sensor) messages such as a special instruction for a certain node is not considered.

In this paper, we propose a potential-based downstream routing protocol (PBDR) for multi-sink wireless sensor networks. In existing PBUR protocols, there is a possibility that some sensor nodes have the same potential since the height of the potential field depends on only the hop count to the sink. Thus, when the sink node transmits data intended for a certain sensor node along the potential field gradient, the data will not always arrive at the destination. In PBDR, multiple sink nodes individually construct potential fields, and all nodes have a set of potentials. The set of potentials are treated as virtual coordinates that identify a destination node. Then, we define a virtual distance between virtual coordinates. A node with data to be sent calculates the virtual distances between the intended destination node and its neighbor nodes, and then forwards the data to the neighbor node closest to the destination node in terms of virtual distance.

We evaluate the data delivery ratio of PBDR at various node densities and packet error ratios, and we use computer simulations to show the protocol's robustness against the failure of multiple sensor nodes or the failure of a sink node.

The rest of this paper is organized as follows. We start by giving an overview of related work in Section II. In Section III, we show the existing potential based routing protocol. We present the proposed PBDR protocol in Section IV. Then in Section V, we evaluate the performance of PBDR through simulation experiments. Finally, Section VI gives our conclusions.

II. RELATED WORK

For wireless sensor networks, various any-to-any routing protocols have been studied. In the flooding method and in the gossiping method, messages are relayed on the basis of broadcasts [4, 5]. These methods suffer from a high number of redundant transmissions, particularly when a few nodes in a specific domain are the destinations.

Many studies have been conducted on proactive and reactive routing protocols [6, 7]. In reactive protocols, each node constructs routes in only the case that communication is required. Then, power consumption can be cut when communication is not needed. The delay time, however, is longer for reactive protocols because of their route discovery procedures. This means that reactive protocols are not appropriate for real-time applications. In proactive protocols, end-to-end delay is small. However, there is overhead because all the nodes collect information about links.

 ISBN: 978-1-61208-231-8

Geographic routing protocols allow for communication between two arbitrary nodes [8]. Some equipment for acquiring the precise geographic position is required for these protocols, and all the nodes must know the position of their destinations. The virtual coordinate assignment protocol (VCap) is able to route data using virtual position without GPS devices [9]. In VCap, all nodes have three shortest hop counts from three anchor nodes and use them as virtual coordinates. Note that since the hop count is an integer, some nodes may have the same virtual coordinate in VCap.

In this paper, we propose a downstream routing based on PBUR. We give an outline of PBUR in the following section.

III. Existing Potential-Based Upstream Routing Protocols

PBUR protocols are categorized as proactive routing protocols. In PBUR, all the nodes have a scalar potential that constructs a potential field. Each node updates its potential based on local information, such as potentials, its residual energy and that of its neighbors, or hop counts to a sink node. A sensor node whose hop count to a sink is smaller (larger) has a higher (lower) potential. Each node with data to be sent forwards the data to a node whose potential is higher than its own, and then the data ultimately reach the sink node. Moreover, load balancing and extending the lifetime of wireless sensor networks by using the residual energy of neighbor nodes or the amount of traffic has been studied [1, 3]. Controlled potential-based routing (CPBR [10]) constructs a potential field for multi-sink wireless sensor networks by using a discrete form of the diffusion equation (1). $\phi(n,t)$ describes the potential of node n at time t. $Z(n)$ is a set of neighbor nodes of node n and $|Z(n)|$ is the cardinality of the set $Z(n)$. A parameter ϵ changes the magnitude of influences by potentials of the neighbor nodes. It is noteworthy that potentials may oscillate when ϵ is larger than one. In CPBR, ϵ is set to the value between 0 and 1 in order to keep the potential from oscillating.

$$\phi(n,t+1) = \phi(n,t) + \frac{\epsilon}{|Z(n)|} \sum_{k \in Z(n)} \{\phi(k,t) - \phi(n,t)\}. \quad (1)$$

In existing PBUR protocols, there is the possibility that some sensor nodes have the same potential. Therefore, when the sink node transmits data to a certain sensor node along the gradient of the potential field constructed through existing PBUR protocols, the data will not always arrive at the destination. This problem is treated as a contour problem as shown in Figure 1. The contour problem is the problem that no node can determine the next hop because no node knows the geographic direction to the destination node by potentials.

In this study, we focus on the advantages of PBUR for wireless sensor networks and implement downstream routing by extending PBUR. As described in subsequent sections, we use the method in CPBR for constructing the potential field, but our method is also applicable to existing PBUR protocols.

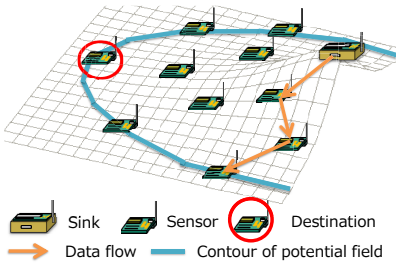


Figure 1. Contour problem for downstream routing using an existing potential construction method

IV. Potential-Based Downstream Routing

PBDR must accomplish the following three tasks in order to handle the contour problem.

1) Assign potentials to all sensor nodes for identifying them
2) Inform the sink nodes of the potentials
3) Route data to a destination node by using its potential as an identifier

In a following PBDR algorithm, we suppose that all sinks can communicate with each other via the local area networks or the Internet.

A. Overview of PBDR

For realizing PBDR, it is first necessary to assign potentials to all sensor nodes in order to identify them. We denote such a potential as P_{id}, and we give an overview of PBDR with P_{id} below.

1) Each sensor node calculates its own P_{id}.
2) When a sensor node generates an upstream data packet, it includes its P_{id} in the packet header, and a sink node records the P_{id} when it receives the upstream data.
3) We define a function $Dist_p(n_1, n_2)$ which is a virtual distance between nodes n_1 and n_2 and is calculated from their P_{id}s.
4) A sensor node with downstream data to be transmitted forwards data to the neighbor node whose distance to the destination node is smallest, as shown by the value of function $Dist_p(n_1, n_2)$. In this way, the data ultimately reaches the destination node.

B. Node Identification

In protocols based on existing methods for constructing a potential field, downstream data will not always arrive at the destination node because of the contour problem. Thus, we assign a virtual coordinate to all sensor nodes in order to identify them. This method is based on the idea of the trilateration. N sink nodes individually construct potential fields, and all nodes have a set of potentials as a virtual coordinate. Here, as in reference [10], the diffusion equation is used by sink node i to construct the potential field F_i $(i = 1, \cdots, N)$. Now, we can define that P_{id} is a set of N potentials. If there are three sink nodes and three potential fields, PBDR can be realized. However, in Section V, we use four sink nodes and four potential fields in order to acquire the redundancy when a sink node fails.

 ISBN: 978-1-61208-231-8

Equation (2) is used to construct the potential field F_i having potential $\phi(n,t,i)$ at node n and time t. ϵ is a constant which plays the same role as the ϵ in the equation (1).

$$\phi(n,t+1,i) = (1-\epsilon)\cdot\phi(n,t,i) + \frac{\epsilon}{|Z(n)|}\sum_{k\in Z(n)}\phi(k,t,i). \quad (2)$$

Generally, in the diffusion equation, when all boundary conditions have the same value, all values in the field converge on the value of the boundary conditions, and the field eventually becomes flat. Consequently, potential routing does not work because there is no gradient in the field without a boundary condition. So, we use equation (3) as a boundary condition so that the potentials of the entire network do not converge on the potential of a sink node. S is a set of sink nodes. Note that sink node i constructs the potential field F_i.

$$\forall s \in S, \phi(s,t,i) = \begin{cases} \phi_{max} & \text{if } i = s \\ \phi_{min} & \text{otherwise.} \end{cases} \quad (3)$$

C. Downstream Routing

To send a data to a specific sensor node, sink nodes must know P_{id} of a destination node. In this paper, we assume that every sensor node uses the potential field whose potential is the highest in its P_{id} in order to periodically send a monitored data packet to the nearest sink node. Each sensor node inserts its P_{id} into the header of the packet and sink nodes can collect P_{id} for every sensor node. In this manner, downstream routing is realized by simultaneously performing upstream routing.

We assume that all the sink nodes are connected to each other with a high speed link. Also, a downstream data packet can be routed to the sink node closest to a destination node and the sink node can start delivery of downstream data.

We define potential distance as a virtual distance calculated from P_{id}. To select a next hop, node n calculates the potential distance $Dist_p$ between its neighbor $k(\in Z(n))$ and destination node d:

$$Dist_p(k,d) = \sqrt{\sum_{i=1}^{N}\left(F_i(k) - F_i(d)\right)^2}. \quad (4)$$

$F_i(k)$ is the potential of node k on the potential field F_i, and $F_i(d)$ is the potential of destination node d. We use potential distance as a routing metric.

A sink node includes P_{id} of destination node d in the header of a downstream data packet, and relay nodes forward the data to node y that fulfills the following condition:

$$y = \arg\min_{k\in Z(n)} Dist_p(k,d). \quad (5)$$

When a data reaches a neighbor node of destination node, the data is forwarded to the destination node using a node ID.

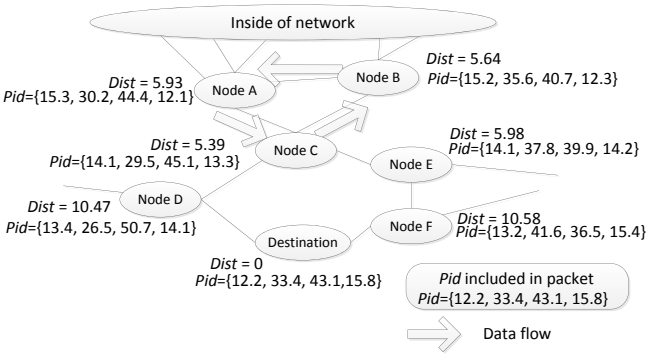


Figure 2. Local-minimum problem

D. Local-Minimum Problem

When a destination node is in a domain that has low node density, for example, at the boundary of a monitoring area, the local-minimum problem may occur. The local-minimum problem arises when a node cannot forward data anywhere, because low node density can lead to void areas and there is no neighbor node closer to the destination node in terms of potential distance.

In the example shown in Figure 2, node C must forward data to node D so that the destination node receives the data. However, $Dist_p(\text{node } D, \text{destination})$ is larger than $Dist_p(\text{node } B, \text{destination})$ and node C does not forward data to node D. We use a local detour rule, in which node v forwards data to node w having the smallest $Dist_p(w, \text{destination})$, even if $Dist_p(v, \text{destination})$ is smaller than $Dist_p(w, \text{destination})$, and node v does not forward data to node u after node v receives the data from node u. According to this rule, node C forwards the data to node B. As a result, a data packet will follow a loop through node A, node B, and node C.

The local-minimum problem occurs when a destination node is near the boundary of the monitoring area, where the node density is low and there is a void area. So we assume that a destination node is near the boundary of the monitoring area when a loop is detected, and we resolve the local-minimum problem by using an alternative routing metric.

Because the height of potential can be treated as a virtual distance from a sink node, a loop is hard to occur when a single potential field is used for downstream routing. So, we use a single potential field when a loop is detected. The node near the monitoring area boundary is located in the area farthest from a certain sink node and the potential of the destination node on the potential field built by the sink node is nearly equivalent to $\phi_{\min}$. Thus, a possibility that the data packet gets close to the boundary of the monitoring area is high when a node forwards the packet to the node farthest from the sink node. In order to send data to the boundary of the monitoring area, we use only one potential field whose potential is the smallest in P_{id} of the destination node. From the above, we define a potential gap $Gap(k,d)$ (6), and use it as an alternative routing metric when a routing loop is detected. Node d is a destination node, and node k is a neighbor of the node that detects a routing loop. The node

 ISBN: 978-1-61208-231-8

that detects the routing loop forwards the data to the node whose potential gap with respect to the destination node is the smallest.

$$Gap(k,d) = |F_i(k) - F_i(d)|, i = \underset{1 \le j \le N}{\arg\min} F_j(d). \quad (6)$$

For example, in Figure 2, potential gap of Node A is 3.1, one of Node C is 1.9 and one of Node D is 1.2. Then, Node C forwards the data to Node D and the data reaches the destination node.

A sequence number and a loop flag are included in the data packet header and are used to detect routing loops. When a node receives a downstream data packet, the node records the sequence number of the data. When a node receives data with the same sequence number, the node judges that a loop has occurred and sets the loop flag to 1. Each node records $n_{history}$ sequence numbers of received packets from the newest one. The routing protocol is shown below for when a loop is detected.

1) Node n checks whether it has recorded a sequence number of the data. If node n detects a loop, it executes process 2. Otherwise, it executes process 3.
2) Node n sets a loop flag to 1 indicating that the data packet is in a loop and executes process 4.
3) Node n sets a loop flag to 0 indicating that the data packet is not in a loop and executes process 4.
4) When a node receives a data packet destined for another node, the receiving node checks this flag in the data. If the flag is set to 1, Gap is used; if the flag is set to 0, $Dist_p$ is used. However, if the flag is set to 1 and there is no node that has a potential gap of less than a potential gap the receiveing node has with respect to the destination node, the receiving node clears the flag.

E. MAC Layer Protocol

In this paper, we use intermittent receiver-driven transmission (IRDT) for the MAC layer protocol [11]. In IRDT, all nodes sleep and wake up asynchronously with the duty cycle $T_{dutycycle}$. Whenever a node wakes up, it sends an ID message that informs neighbor nodes that the node is ready to receive data.

When node n_1 forwards data to node n_2 in IRDT, the procedure shown in Figure 3 is used. Node n_1 with data to be sent wakes up and waits for an ID message from node n_2. Upon receiving an ID message from node n_2, node n_1 sends an SREQ message informing node n_2 that it has a data packet for node n_2. When node n_2 receives the SREQ message, it stays awake and sends to node n_1 a RACK message, which is an acknowledgement for communication request. After that, node n_1 sends a data message to node n_2. Finally, node n_2 sends to node n_1 a DACK message, which is an acknowledgement for data. If node n_2 is not a destination node, node n_2 becomes a sender and waits for an ID message from a neighbor node.

Node n_1 drops the data when forwarding the data does not succeed within $T_{timeout}$ after node n_1 woke up. Also, when the number of forwards exceeds time to live (TTL), node n_1 drops the data.

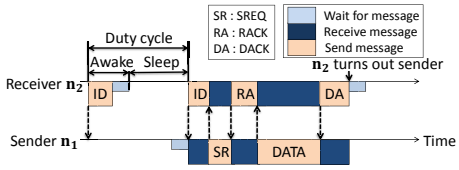


Figure 3. Procedure for forwarding data in IRDT

Table I
SIMULATION CONFIGURATION

Parameter	Value
Radio range	100 m
Time to live (TTL)	15
Data packet size	128 byte
Bandwidth	100 kbps
$\phi_{\max}$	90
$\phi_{\min}$	0
ϵ	0.8
$T_{dutycycle}$	1 s
T_{update}	50 s
$T_{timeout}$	5 s
$n_{history}$	3

V. SIMULATION EXPERIMENTS

In this section, we present the results of our simulation experiments. PBDR is implemented in the OMNeT++ [12] network simulator. We evaluate data delivery ratio of PBDR at various node densities and packet error ratios, and show its robustness against sensor-node failure and sink-node failure.

The sensor nodes are randomly distributed in a 600 m $\times$ 600 m square. In this network, the number of deployed sensor nodes is from 50 to 250 and 4 sink nodes are situated at the four corners of observation area. In the data generation model, the rate of data generation is $\frac{1}{100}$ per node for upstream communication and $\frac{1}{300}$ per node for downstream communication in Poisson process. The reason that the rate of data generation is higher for upstream communication than for downstream communication is that downstream communication is demanded less frequently. Under these conditions, we evaluate how the data delivery ratio is affected by node density and packet error rate (Section V-A), by sensor nodes failure (Section V-B), and by sink node failure (Section V-C). The details of the simulation configuration are summarized in Table I.

A. Node Density

Simulation results are shown in Figure 4 for changing the packet error rate from 0 to 0.4. The horizontal axis shows the number of nodes, and the vertical axis shows the data delivery ratio. The number of trials is 50, and the confidence interval is 95%.

The data delivery ratio is low when the node density is low because there are few links in the entire network and the local-minimum problem easily occurs. The data delivery ratio increases when the node density is high because the number of links in the entire network increases. When the node density is excessively high, however, packet collisions occur frequently, thus decreasing the data delivery ratio. The data delivery ratio is highest when the number of nodes is 150. In that case, the data delivery ratio is 99.5% and the average number of neighbor nodes is 16.7.

 ISBN: 978-1-61208-231-8

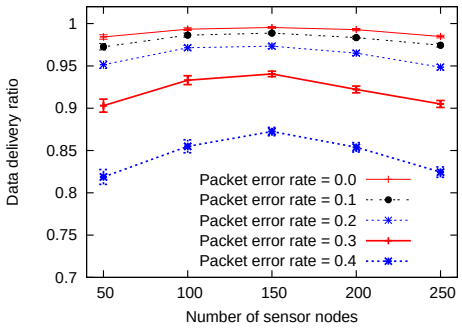


Figure 4. Data delivery ratio vs node density

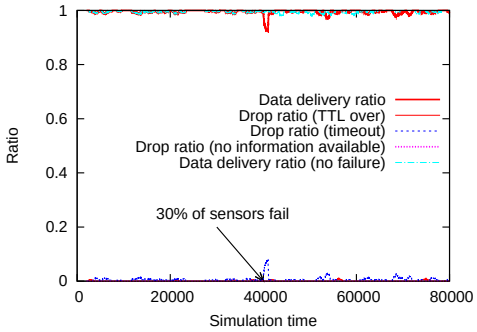


Figure 5. Data delivery ratio and drop ratio (sensor nodes failure)

B. Failure of Sensor Nodes

In the case that there are 150 nodes and 45 sensor nodes fail, we evaluate the data delivery ratio from $t - 1000$ s to t at each time t. The simulation time is 80,000 s and 45 sensor nodes fail after 40,000 s have elapsed. The number of trials is 10.

Figure 5 shows the data delivery ratio and drop ratio from $t - 1000$ s to t at each time t. The drop ratio (TTL over) is the packet drop ratio when the number of forwards of the data is over TTL. The drop ratio (timeout) is the packet drop ratio when a node with a data packet cannot forward the data within $T_{timeout}$ after the node wakes up. The drop ratio (no information available) is the packet drop ratio when no sink node has P_{id} of a destination node. The results show that downstream routing works well even if sensor nodes fail.

The data delivery ratio decreases steeply when sensors fail at 40,000 s, but quickly recovers to the level observed before node failure. The drop ratio (TTL over) and no information available do not change considerably when sensor nodes fail, but the drop ratio (timeout) increases steeply. After node failure, data packets are dropped more frequently by time out. This is because the number of links in the entire network decreases and the load on the entire network increases after sensor nodes fail.

C. Failure of Sink Node

In the case that there are 150 nodes and one of the four sink nodes fail, we evaluate the data delivery ratio at immediately prior to 1,000 s. The simulation model is the same as one for sensor nodes failure. When sink node s fails, all the potentials of F_s converge on $\phi_{\min}$ because of boundary condition 3. A sensor node with upstream data to be sent decides the next hop according to the potential field whose value is highest among the potentials. In this manner, the other three sink nodes collect P_{id} for each sensor node and PBDR regains its effectiveness after sink node failure.

Figure 6 shows changes in potential until the potential fields converge. Here, the changes in potential for three nodes are shown. The first is the farthest from the failed sink node, with a hop count to the failed sink node of 7. The second is deployed near the center of the network, with a hop count to the failed sink node of 4. The third is a 1-hop neighbor of the failed sink node. In Figure 6(b), the changes of the potential field that were constructed by the failed sink node are shown and the potentials converge on $\phi_{\min}(= 0)$ in about 30,000 s. In Figures 6(a), 6(c), and 6(d), the changes in the potential fields that the other three sink nodes construct respectively are shown and the potentials converge in about 20,000 s.

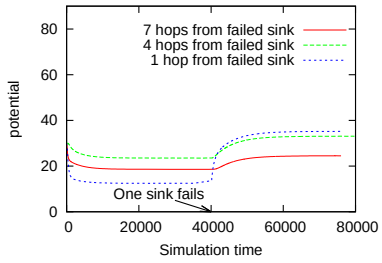
The data delivery ratio and drop ratio at just before 1,000 s in each cases is shown in Figure 7. These results show that downstream routing works well, even if one of four sink nodes fails. When a sink node fails at 40,000 s, the data delivery ratio sharply decreases temporarily and increases again. This is because the other three sink nodes lack the P_{id} of sensor nodes which failed sink node held, and the drop ratio (no information available) become temporarily high. After a sink node fails and the other three sink nodes collect potential information about all sensor nodes, the drop ratio (no information available) decrease. However, data are dropped by time out more frequently. This is because, when a sink node fails, it becomes necessary for the upstream flow to be processed by three sink nodes instead of four and the load on the entire network increases accordingly. We note that the data delivery ratio increases more quickly than the time of potential convergence which is about 20,000s.

VI. Conclusion and Future Work

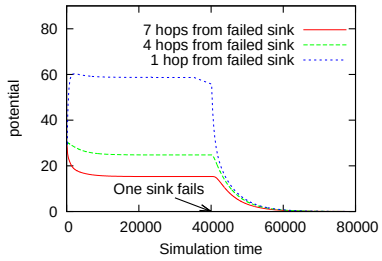
In PBDR, multiple sink nodes construct independent potential fields and all nodes have a set of potentials used as a virtual coordinate. We defined virtual distance based on virtual coordinates and use it as a routing metric. Through OMNeT++ simulation, we evaluated the data delivery ratio for various node densities and packet error rates, as well as the robustness against failure of multiple sensor nodes or of a sink node. PBDR achieves a data delivery ratio greater than 99.5% when the network has a suitable node density. Even if multiple sensor nodes fail or a sink node fails, the data delivery ratio recovers immediately after sensor-node failure or sink-node failure.

In PBDR, when the number of potential field increases, reliability of downstream routing can be raised, but overhead also increases. Hence, we plan to investigate this tradeoff in future work. In this paper, we do not consider power consumption. So, we will evaluate the distribution of power consumption using the method for constructing the potential field with load balancing.

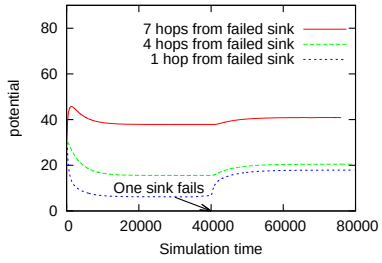
 ISBN: 978-1-61208-231-8



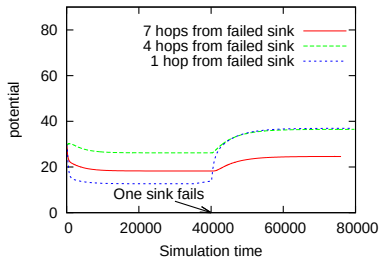
(a) potential F_0



(b) potential F_1 (constructed by failed sink node)



(c) potential F_2



(d) potential F_3

Figure 6. Potential convergence after sink-node failure

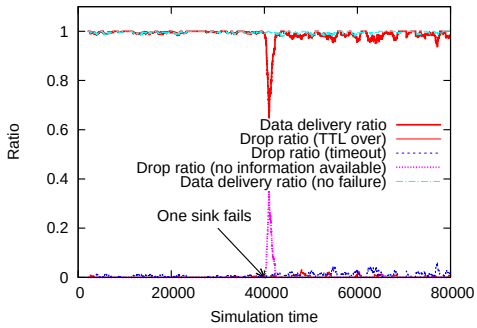


Figure 7. Data delivery ratio and drop ratio (sink node failure)

ACKNOWLEDGMENT

This research was supported in part by "Grant-in-Aid for Scientific Research (C) 23500097 and for JPSP Fellows (24738)" of the Japan Society for the Promotion of Science (JSPS) in Japan.

REFERENCES

[1] C. Wu, R. Yuan, and H. Zhou, "A novel load balanced and lifetime maximization routing protocol in wireless sensor networks," in *Proceeding of IEEE Vehicular Technology Conference*, May 2008, pp. 113–117.

[2] A. Basu, A. Lin, and S. Ramanathan, "Routing using potentials: a dynamic traffic-aware routing algorithm," in *Proceedings of ACM SIGCOMM 2003*, Aug. 2003, pp. 37–48.

[3] H. Liu, Z.-L. Zhang, J. Srivastava, V. Firoiu, and B. DeCleene, "PWave: flexible potential-based routing framework for wireless sensor networks," in *Proceeding of IFIP/TC6 Networking Conference*, May 2007, pp. 14–18.

[4] S. Guo, Y. Gu, B. Jiang, and T. He, "Opportunistic flooding in low-duty-cycle wireless sensor networks with unreliable links," in *Proceedings of ACM MobiCom 2009*. New York, NY, USA: ACM, Sep. 2009, pp. 133–144.

[5] S. Fauji and K. Kalpakis, "A gossip-based energy efficient protocol for robust in-network aggregation in wireless sensor networks," in *Proceedings of IEEE Pervasive Computing and Communications Workshops*, Mar. 2011, pp. 166 –171.

[6] T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, A. Qayyum, and L. Viennot, "Optimized link state routing protocol," *Internet Draft draft-ietf-manet-olsr-txt Work in progress*, pp. 1–15, Apr. 2003.

[7] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of IEEE Mobile Computing Systems and Applications*, Feb. 1999, pp. 90–100.

[8] L. Shu, Y. Zhang, L. Yang, Y. Wang, M. Hauswirth, and N. Xiong, "TPGF: geographic routing in wireless multimedia sensor networks," *Telecommunication Systems*, vol. 44, pp. 79–95, Oct. 2010.

[9] A. Caruso, S. Chessa, S. De, and A. Urpi, "GPS free coordinate assignment and routing in wireless sensor networks," in *Proceedings of IEEE INFOCOM 2005*, Mar. 2005, pp. 150–160.

[10] D. Kominami, M. Sugano, M. Murata, and T. Hatauchi, "Controlled potential-based routing for large-scale wireless sensor networks," in *Proceedings of Modeling, analysis and simulation of wireless and mobile systems*, Jan. 2011, pp. 187–196.

[11] C. Damdinsuren, D. Kominami, M. Sugano, M. Murata, and T. Hatauchi, "Lifetime extension based on residual energy for receiver-driven multi-hop wireless network," in *Cluster Computing*, May 2012. [Online]. Available: http://dx.doi.org/10.1007/s10586-012-0212-0 [retrieved: October, 2012]

[12] A. Varga, "OMNeT++," in *Modeling and Tools for Network Simulation*. Springer Berlin Heidelberg, Oct. 2010, pp. 35–59.

 ISBN: 978-1-61208-231-8

Link Design for Multi-hop Underwater Optical Wireless Sensor Network

Zahir Ahmad and Roger Green
School of Engineering
University of Warwick
Coventry CV4 7AL, UK
e-mail: Z.U.Ahmad@warwick.ac.uk, and roger.green@warwick.ac.uk

***Abstract*—This paper presents a link designed for a multi-hop underwater optical wireless communication system using green/blue Light Emitting Diodes (LEDs). The proposed system can increase the communication distance using multi-hop communication compared to single hop communication. The suggested system uses very simple and inexpensive hardware to build a cost effective solution. The established link can support a bandwidth up to 100 KHz for a communication range up to 1 meter without using any external optics and without degrading the required signal to noise ratio.**

Keywords-underwater; optical wireless; sensor network; visible light.

I. INTRODUCTION

More than two thirds of world's surface is covered by water and this area is still mostly undiscovered by human beings. One efficient and reliable communication system is the first step towards the invention of this huge underwater world. Until now, most underwater communication is based on either wired or acoustic technology. Wired technology has its limitation in terms of installation, maintenance and mobility. For short and medium range applications, wireless is the suitable solution especially underwater, where the medium is very rough and harsh. So far, acoustic methods are the dominant underwater communication system used for long range low bandwidth links, because sound propagates very well underwater compared to other waves. However, the limitation of acoustic communication is the lack of bandwidth to support high speed communications, for example, sound can propagate up to a few kilometers with a speed of 1500m/s, which is not enough for many applications. Time-varying multipath propagation and low speed of sound underwater produces a very poor and high latency communication channel, which cannot support real time data transfer such as audio/video. Moreover, the cost of acoustic components is very high and the dimensions of components are very large. All those limitations of acoustic communication have stimulated researchers to find a cheap alternative for underwater communication system capable of allowing high bandwidth for real time applications.

In this paper, a multi-hop static underwater optical wireless communication network using visible light has been proposed. Multi-hop communication is a well-known technique in free space communication for spatial reuse which was also proposed by many researchers for underwater optical wireless communications. In this process, intermediate nodes relay the information and control signals to the gateway node which ultimately stores and sends data to the base station.

The rest of the paper is organized as follows: Section II reviews the background and related work. In Section III, some of the issues related to underwater optical wireless communication are described. The system design procedure is described in Section IV, followed by performance analysis in Section V. Finally, conclusion and future work are illustrated in Section VI.

II. BACKGROUND AND RELATED WORK

Several research groups are actively investigating different aspects of underwater optical wireless communication systems, starting from channel characterization to system design. The water medium itself is a complex medium and light propagation varies in different types of water at different depths [1], so it is not an easy option to find a generic channel model for all types of water. Since underwater optical wireless is a relatively new research area, most of the work until now has focused on unidirectional single hop communication, implemented either by software or hardware, and also some groups are investigating sensor applications. Vasilescu *et al* at MIT have built an underwater sensor network using visible light but have used an optical wireless link only to upload the data from a sensor node to an Unmanned Aerial Vehicle (UAV) [2]. An unidirectional optical wireless link capable of sending data at 320Kbit/s up to a distance of 2.2m for an underwater sensor network was presented in [2]. To achieve this communication distance, a high powered LED array was used, and this link was only used to upload the sensor data from sensor node to an Autonomous Underwater Vehicle (AUV). The same group advanced their research to achieve a data rate of 1.2Mbit/s for a communication range of 30m. Recently, they reported a bi-directional communication system to achieve a communication range of 50m [3]. They used very high power LEDs and expensive optics to obtain these results.

Chancery designed and tested an FM optical wireless communication system for underwater which was capable of sending data at 10Mbps rate [4]. Later, his work was advanced by Cox, Simpson and Everett to investigate the various fundamental issues like modulation techniques, error correction, high speed communication channels, etc. [5][6][7] .

 ISBN: 978-1-61208-231-8

Anguita *et al.* are working on diffuse underwater optical wireless sensor network using a planner transceiver [8], but they are concentrating on integration of free space technology with underwater. They have achieved a 100 Kbps data rate in a communication distance of 1.8m.

Norman and the group at Woods Hole Oceanographic Research Center have reported a high bandwidth communication link of 5Mbps over a distance of 200m in clean water using a diffuse optical communication link [9]. They used both green and blue light to make the system bidirectional, and an acoustic modem to wake up the sea floor installation [10].

Amongst others, Felix reported an underwater communication system using the IrDA physical layer with 3Watt, high-power LEDs [11]. Frank proposed a laser-based communication link which achieved a data rate of 1Gbit/s over a distance of 2m in a laboratory water pipe, and predicted that up to 48m could be achieved in clear water [12]. A cost effective underwater optical modem has been proposed by Feng to achieve a communication distance up to 10 meters [13]. Sermask modeled the underwater optical wireless channel using vector radiative transfer theory to investigate the multiple scattering and polarization of light [14]. He calculated the bit error rate of On-Off-Keying modulation, and 4-level amplitude modulation with different FOV. Arnon proposed three types of communication links and analyzed the performance of each type [15]. From his analysis it is seen that the communication performance decreased rapidly when water absorption increased, but a high data rate was still possible.

III. ISSUES RELATED TO UNDERWATER OPTICAL WIRELESS SENSOR NETWORK

In this section, some of the fundamental issues related to underwater optical wireless and adopted network architecture are discussed.

A. Which spectrum range to select?

An underwater optical wireless channel suffers from both scattering and absorption, resulting in severe attenuation. Behavior of light in water depends on the water components. Sea water is primarily composed of H_2O, but it also has different salts, such as $NaCl, MgCl_2, Na_2So_4, KCl$ etc., which absorb light at specific wavelengths. Equation (1) describes the relation between attenuation and communication distance,

$$A = e^{-k(d_1 - d_2)(\frac{d_1}{d_2})^2} \quad (1)$$

where the transmitter and receiver are placed at *d1* and *d2*, and *k* is the attenuation coefficient defined as:

$$k = \alpha(\lambda) + \beta(\lambda) \quad (2)$$

Here, α is the absorption coefficient which depends on the light wavelength, and β is the scattering coefficient which mainly depends on wavelength as well as the turbidity of water.

From the basics of light propagation in water, it is found that the best wavelengths which propagate in water are in the green-blue region of the visible spectrum (wavelength 400-550nm), and so two wavelengths within this range have been selected for the communication system to be described.

B. Modulation techniques

Modulation techniques play a vital role in all sorts of communication systems including optical wireless. Three major characteristics of modulation techniques are transmission efficiency, power efficiency and bandwidth efficiency. A modulation technique with high bandwidth efficiency ensures that the overall system bit rate is high; on the other hand side, power efficiency is needed for longer life time of the system when run from local finite sources. Two most common modulation schemes used in optical wireless are On-Off-Keying (OOK), and Pulse Position Modulation (PPM).

On Off Keying (OOK) is the simplest form of modulation in terms of implementation. Here, the optical power is directly modulated by varying the source current in sympathy with the data, whereas on the receiver side the detector produces a photocurrent proportional to the received photons. OOK can be either in the form of Non Return to Zero (NRZ), or Return to Zero (RZ). In this paper, NRZ-OOK signaling is used because of lower power requirements.

As mentioned, in PPM the position of the pulse is changed during a temporal cycle to represent a different bit. In this method the average power requirements are decreased compared to OOK, in compensation for an increase in bandwidth requirements. PPM can be either in two, or multi-level, depending on the requirement, where it is represented by L-PPM.

The proposed design has considered NRZ-OOK modulation techniques because of the simplicity of implementation and lower power requirement.

C. Proposed Network architecture

Two possible network architectures for underwater communication are presented in Figure 1.

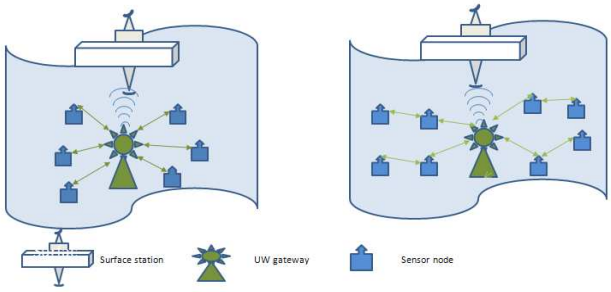


Figure 1. Underwater optical wireless network architecture

In the first scenario, a star network topology is presented, where sensor nodes send information via an optical link to a gateway station which can be located on the surface or under the water. The underwater gateway station stores information from all nodes in the cluster and sends it

to the surface station periodically. Another scenerio presented on the right hand side of the above figure is based on a tree topology, where each node relays the information to the next node, and the surface station receives all node information via its nearest sensor nodes. Both these architectures have some advantages and limitations, for example, in the first case protocol development will be easier since the total communicaton system is based on one hop communication, and it will have lower power consumption because, after passing the data to gateway nodes, each node can go to the sleep state. This type of architecture has limitations in terms of distance covered. On the other hand, a tree-based multi-hop architecture has the advantage of covering a large geographical area. Multi-hop comunication needs a complex routing protocol, since each node needs to know its neighbour to forward information, especially in the mobile environment. Since the focus of this work is to build a static and directional sensor network, this problem can be easily solved by using hop-by-hop routing.

D. *Physical layer development*

The possible physical layer architectures of the network are shown in Figure 2. As seen, it can be implemented in different ways. First of all, a simplex communication is possible where each sensor node just forwards sensor information through the optical wireless link to the gateway station. In this case, the gateway node gives a command to the sensor node by using another medium, for example, in an acoustic link. So, this is not fully optical communication, but rather a hybrid communications approach. Having both optical and acoustic hardware increases the overall system complexity, especially when the cost of suitable higher bandwidth acoustic modems is high.

Another approach is presented in figure 2 (b), where both up- and downlinks are designed using the same colored LED. In this approach, a half-duplex communication can be achieved, which means a lower throughput for the system.

The implementation which is being described here utilizes a full-duplex communication model using two different colored LEDs. Compared to the half-duplex system, it has greater bandwidth efficiency at almost the same complexity. Only a pairing of a green and a blue transceiver has to be done correctly to make the system work properly.

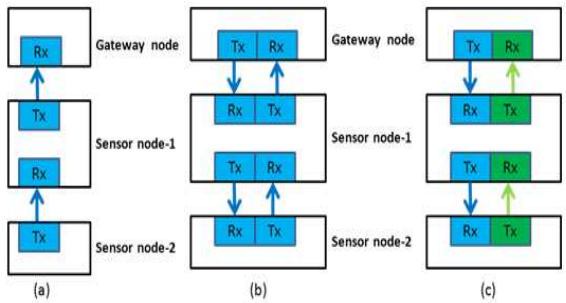


Figure 2. Physical layer structure of the multi-hop underwater optical wireless sensor network a) Simplex, b) Half-duplex, and c) Full duplex

IV. SYSTEM DESIGN

Free space optical wireless communications is dominated by infrared technology which cannot be used underwater. As discussed in the previous section, the best wavelengths suitable for underwater communication are in the green/blue part of the spectrum, so whole system is designed accordingly.

A. *Components selection*

An LED and a photodiode are the two main components which need to be selected carefully for best performance. After careful consideration, an Avago HLMP LED was selected which is available both in green and in blue. The power dissipation of this device is about 116 mW and the viewing angle is 15 degrees.

A SILONEX SLD-70BG2 photodiode was chosen for the receivers which has peak sensitivity in the green spectral region. Compared to other silicon photodiodes available in the visible spectrum range, it has less capacitance (180pF) and higher active region (9.8 sq.mm).

B. *Transmitter circuit*

To transmit a digital signal, a relatively simple digital optical wireless transmitter circuit was used with the selected LED as shown in Figure 3 to provide OOK signals.

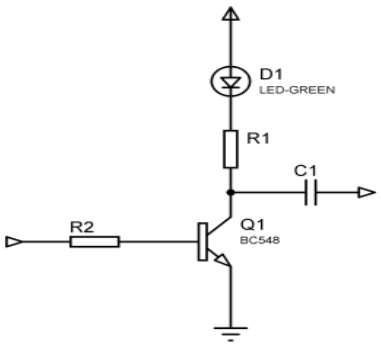


Figure 3. Digital optical wireless transmitter

C. *Receiver circuit*

The receiver can be the more complicated part of an optical wireless system design. There are a few common receiver design architectures which are mostly preferred by researchers. Amongst them, the bootstrap front end and transimpedance front end are frequently used. The target of all configurations is to increase the bandwidth and sensitivity by minimizing the photodiode's capacitance effects. For the high bandwidth applications, the bootstrap configuration is preferred, whereas for better gain, the transimpedance configuration has advantages over the bootstrap approach. After investigating both the receiver techniques, a simple form of transimpedance front end circuit using a single transistor, as shown in Figure 4, was used for the proposed system.

 ISBN: 978-1-61208-231-8

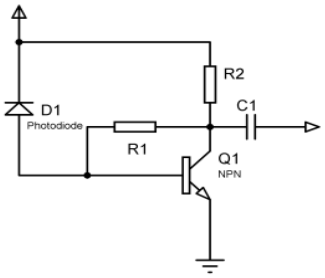


Figure 4. Modified transimpedance receiver front end

The bandwidth of the transimpedance system can be determined by the following equation,

$$f = \frac{1}{2\pi R\left(\frac{C_D}{A} + C_{bc}\right)} \qquad (3)$$

Where, R = load resistance, C_D = Device capacitance, C_{bc} = transistor base emitter capacitance and A = open loop amplifier gain.

As seen, the device capacitance is reduced in significance considerably due to the high gain, A, of the amplifier, but the base-collector capacitance effects cannot be similarly minimized.

V. PERFORMANCE ANALYSIS AND DISCUSSION

Performance analysis of the designed receiver has been done in terms of gain, bandwidth, and noise characteristics. To estimate the performance, all the experiments were carried first in air and then through water to compare the performance analysis.

A. Gain of the transceiver in air

As seen in Figure 5, the received signal decreases continuously when communication distance increases, understandably, because of the weakening optical power incident on the photodiode. Conversely, the greatest signal is achieved when the transmitter and receiver are around 1 cm apart. Overall, when the distance between transmitter and receiver is about 80 cm, the channel loss is about 48 dB. In this project, the target communication range is about 60 cm, where corresponding loss is around 45 dB.

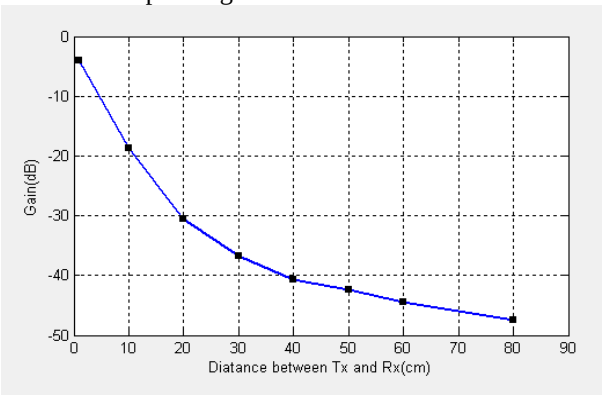


Figure 5. Link gain in different communication range

B. Bit-rate of the transceiver

The achievable bit rate of the designed transceiver has been estimated from Figure 6. With the digital transmitter, finding the achievable bandwidth of the system was undertaken using the maximum bit rate the system can convey.

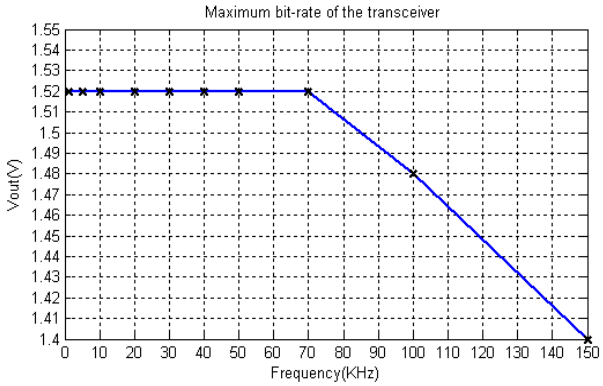


Figure 6. Maximum possible bit-rate of the transceiver

C. Noise performacne in air

Finding signal to noise ratio experimentally in an optical wireless system is challenging due to the effects of ambient light in respect of shot noise in the detector, thermal noise in the input resistances (especially the load resistor), and the masking effect of the ambient itself. Here, the average peak-peak value of the signal and noise was measured, and signal to noise ratio was calculated from the following equation:

$$SNR = 20\log\frac{(S+N)_{Pk-Pk}}{N_{Pk-PK}} \qquad (4)$$

Where $(S+N)_{Pk-Pk}$ is defined as the peak to peak amplitude of the signal with noise and N_{Pk-PK} is defined as the amplitude of the noise voltage. Noise analysis of the system has been estimated in three different scenarios: first of all, the signal to noise ratio was measured in the ideal situation where neither ambient light nor daylight was present. The same measurement was done in the presence of ambient light and in the night environment without any light sources, to find the noise characteristics.

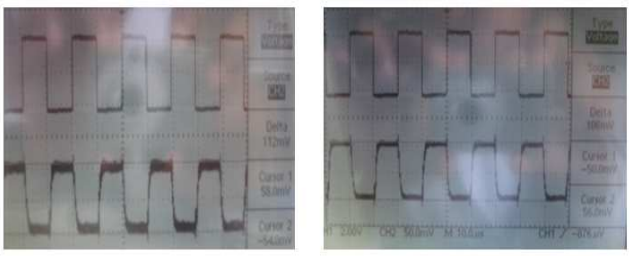


Figure 7. Signal output at the receiver with and without ambient light

Figure 7 shows the output waveform at the receiver with and without ambient light during the day time. As seen, the ambient light has a strong effect on the communication system. The average ambient noise Pk-Pk to value was measured at about 16 mV. A signal to noise ratio of 14 dB

 ISBN: 978-1-61208-231-8

was calculated without the ambient light, and 10 dB with the ambient light.

D. Comparison of air test with water testing

The picture of the water test setup is shown below,

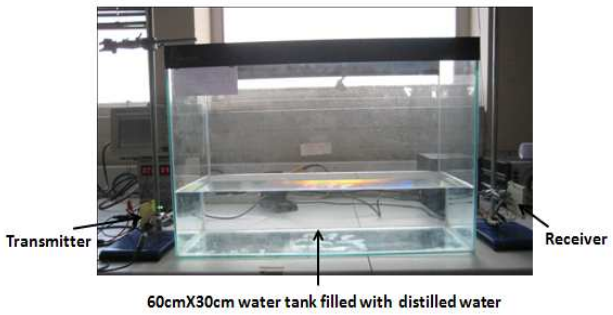


Figure 8. Water test setup

Here, transmitter and receiver are placed on either side of the tank and pointed to each other to measure the gain of the receiver. The tank was made of glass and dimension of the tank is 60cm x 30cm x 45cm. The tank was filled with 20 liters of distilled water and placed inside the experimental laboratory.

To validate the air testing gain of the link has been measured for air and through water for same distance. The output waveform at the receiver can be found in the following figure.

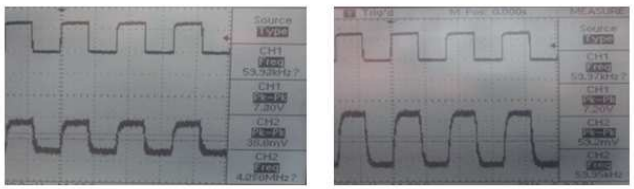


Figure 9. Comparison between output voltage at receiver (Left side through air and Right side through water tank)

As seen, the received output signal voltage was about 40mV for air and about 60mV for water testing for the same distance of 65cm and same frequency of 60 KHz. Because of the glass water tank some light might reflected back from the glass while propagating to the receiver which made for a better gain during water testing. In reality, the gain in water must be lower than the air as water is denser medium than air.

E. Discussion in context of available underwater system

Underwater systems developed by different research groups have different objectives, and chosen components accordingly. For example, Vasilescu *et al.* designed his transmitter with high power LEDs to obtain maximum distance [2]. The radiant power of used LED was 700mW which is much higher compare to LED used for the proposed solution (120mW). It is clear that more optical power will ensure larger distance according to Beer's law. However, the objective of this solution is to design a cost effective system to prove the concept of multi-hop underwater communication, so comparison in terms of distance and bandwidth with other system may not justify the achieved results. The same analogy is true for other systems as well. Anguita *et al.* implemented a planar type transmitter with 12 LEDs to achieve the communication distance of 1.8m [8]. The proposed solution in this paper also works in the 1m range without using any external lenses, and can go beyond few meters if external lenses are used. The same way, other underwater systems can be discussed and compared with the proposed system.

VI. Conclusion and Future Work

An underwater optical wireless communication link has been presented for multi-hop underwater optical wireless communication. Performance analysis of the multi-hop communication system will be undertaken next. As the communication system will be in the form of an amplify-and-forward system, so the expected multi-hop communication performance will be relatively similar to a single hop system, in terms of gain. Moreover, a directional Medium Access Control (MAC) layer protocol is being developed to support the built network for real applications.

Acknowledgment

The authors would like to acknowledge the facilities and support provided by the School of Engineering, University of Warwick.

References

[1] J.W.Giles and I. N. Bankman, "Underwater optical communications systems. Part 2: basic design considerations," in *Military Communications Conference, 2005. MILCOM 2005. IEEE*, pp. 1700-1705 Vol. 3, 2005.

[2] I. Vasilescu, K. Kotay, D. Rus, and P. Corke, "Data collection, storage and retrieval with an underwater sensor network," presented at the *International Conference on Embedded Networked Sensor Systems*, 2005.

[3] M. Doniec and D. Rus, "BiDirectional optical communication with AquaOptical II," in *Communication Systems (ICCS), 2010 IEEE International Conference on*, pp. 390-394, 2010.

[4] A. M. Chancey, "Short Range Underwater Opticlal Communciaiton Links," M.S. thesis, North Carolina State University, Raleigh, NC, 2005

[5] A. J. Simpson, "A 1Mbps underwater communication system using LEDs and Photodiodes with signal processing capability," M.S. thesis, Dept. of Elec. and Comp. Eng, North Carolina State University, Raleigh, NC, 2007.

[6] W. C. Cox, J. A. Simpson, C. P. Domizioli, J. F. Muth, and B. L. Hughes, "An underwater optical communication system implementing Reed-Solomon channel coding," in *OCEANS 2008*, pp. 1-6, 2008.

[7] J. A. Simpson, W. C. Cox, J. R. Krier, B. Cochenour, B. L. Hughes, and J. F. Muth, "5 Mbps optical wireless communication with error correction coding for underwater sensor nodes," in *OCEANS 2010*, pp. 1-4, 2010.

[8] D. Anguita, D. Brizzolara, and G. Parodi, "VHDL modules and circuits for underwater optical wireless communication systems," *WTOC*, vol. 9, pp. 525-552, 2010

[9] C. Pontbriand, N. Farr, J. Ware, J. Preisig, and H. Popenoe, "Diffuse high-bandwidth optical communications," in *OCEANS 2008*, pp. 1-4, 2008.

 ISBN: 978-1-61208-231-8

[10] N. Farr, A. Bowen, J. Ware, C. Pontbriand, and M. Tivey, "An integrated, underwater optical /acoustic communications system," in *OCEANS 2010 IEEE - Sydney*, pp. 1-6, 2010.

[11] S. Felix, Z. U. R., and T. Jochen, "Visible Spectrum Optical Communication and Distance Sensing for Underwater Applications," presented at the ACRA, Australia, 2004.

[12] F. Hanson and S. Radic, "High bandwidth underwater optical communication," *Appl. Opt.*, vol. 47, pp. 277-283, 2008.

[13] F. Lu, S. Lee, J. Mounzer, and C. Schurgers, "Low-cost medium-range optical underwater modem: short paper," presented at the Proceedings of the Fourth ACM International Workshop on UnderWater Networks, Berkeley, California, 2009.

[14] S. Jaruwatanadilok, "Underwater Wireless Optical Communication Channel Modeling and Performance Evaluation using Vector Radiative Transfer Theory," *Selected Areas in Communications, IEEE Journal on*, vol. 26, pp. 1620-1627, 2008.

[15] S. Arnon, "Underwater optical wireless communication network," *Optical Engineering*, January, 2010.

[16] R. J. Green and M. G. McNeill, "Bootstrap transimpedance amplifier: a new configuration," *Circuits, Devices and Systems, IEE Proceedings G*, vol. 136, pp. 57-61, 1989.

 ISBN: 978-1-61208-231-8

Multipath Route Construction Using Cumulative Residual Energy for Wireless Sensor Networks

Saad Rizvi
Electrical and Computer Engineering
University of Manitoba
Winnipeg, Canada
umrizvi@cc.umanitoba.ca

Ken Ferens
Electrical and Computer Engineering
University of Manitoba
Winnipeg, Canada
ferens@ee.umanitoba.ca

Abstract— **This paper presents a novel method for constructing multiple routing paths based on paths which have highest cumulative residual energy. An advantage of selecting the path with highest cumulative residual energy is that it minimizes the probability that nodes along the path will deplete their energy and thus minimizes path failures in the network. The algorithm incorporates a multipath discovery phase without incurring any overhead by "piggybacking" the cumulative residual energy data to existing reinforcement packets of directed diffusion. The algorithm also updates residual energy at the highest rate supported by the network. Simulations show that the proposed method has lower residual energy variance (38%, 30% less) and longer network lifetime (85%, 32% longer) than basic directed diffusion and a load-balanced directed diffusion version which does not implement multipath routes, respectively.**

Keywords-wireless sensor network; energy efficient; directed diffusion; load balancing; cumulative residual energy; braided multipath; network lifetime.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) (due to their low power operation, ease of deployment) have been used for different applications like environmental monitoring, healthcare applications and target tracking [1]. In wireless sensor networking, design of a suitable routing protocol is challenging. In most of its applications the main goal is to maximize lifetime of the nodes in the network. One approach to this problem is to balance the load among all nodes in the network. Since a battery is the only source of energy nodes have, the challenge is to design an effective routing algorithm keeping in mind the goal of maximizing lifetime of the sensor nodes and balancing the load of nodes network wide. Thus, nodes should consume lower energy and load must be balanced to increase network lifetime.

A load balancing algorithm aims to achieve an energy efficient solution for such networks by balancing the work load equally among the nodes in the network. By judicious use of limited available energy, network life time can be extended to the fullest. By considering the network lifetime as the time the first node in the network fails (dies), with load balancing we can think of all nodes being depleted of energy slowly and uniformly causing all nodes to die nearly at the same time. By doing this, one can lower maintenance cost and improve overall performance.

The proposed algorithm utilizes multiple paths between the sink and source nodes to extend the network lifetime by efficiently balancing the traffic load of nodes within the network. Dynamically switching to best path, for routing data towards the sink, not only helps in load balancing but also allows avoiding network failures that may occur at an early stage. This paper attempts to overcome the problem of limited energy resources and unequal energy distribution across the network by proposing this multiple path energy efficient routing algorithm.

The proposed method can be applied to basic directed diffusion (DD) [2] for a large distributed sensor network. Using the basic DD's reinforcement phase, we find the two best paths that have the highest residual energy without incurring any significant overhead. By simply reinforcing the two high cumulative energy nodes, the sink initializes the path discovery phase. Similarly, the reinforced nodes relay the reinforcement by reinforcing their two highest cumulative energy upstream neighbors. This continues until he reinforcement messages reach a source node. Thus, two paths which have the highest cumulative energy from the source to the sink can be constructed.

This paper presents an efficient approach which considers hop count and cumulative residual energy during the data transmission process. The reinforcement message packet (RMP) contains a "cumulative residual energy" field. Each intermediate node during the reinforcement phase adds its own residual energy to the value in this field. When RMPs find the source, the source selects the path with the highest CRE. The rationale behind selecting the path with high CRE is to select a path to support the goals of load-balancing and fault tolerance. This paper implements a multipath routing strategy and incorporates decision making in the source nodes to select a path to provide resilience against node failures. By doing this it was found that load balancing can also be achieved and network lifetime was extended.

The remaining parts of the paper are organized as follows: Section II discusses related work and identifies the extensions and contributions of this work. Section III gives the details of the methods to improve load balancing and fault tolerance among nodes in the network. Section IV discusses the simulation experiments performed to compare the proposed algorithms with other leading algorithms. Finally, conclusions and future work are given.

 ISBN: 978-1-61208-231-8

II. RELATED WORK

For a flat network with high density of homogeneous nodes (i.e., all nodes have same capabilities), the problem of energy consumption and unequal load distribution can be resolved using energy efficient routing protocols. Among the classification of flat, query based routing protocols, Directed Diffusion (DD) has gained importance due to its flexibility, fault tolerance and energy efficiency. Although in its basic form the protocol does not guarantee load balancing, but extensions have been made [3] to make it more efficient. The initial work in [2] has provision for multipath routing to provide protection from path failures but it does not discuss detailed implementation. Since the algorithm constructs path with least-delay, an approach to implement multipath routing can be to construct multiple least delay paths. These multiple paths can then be used either for concurrent data transmission or by selecting the best path for transmitting data. Using a least-delay path, it is not feasible to incorporate load-balancing in the network. Since the least-delay path will have a minimum number of nodes between sink and source, the energy will be consumed at a greater rate by the nodes along this path than others and they will die prematurely. In most routing protocols, a single-path routing strategy is used for data transmission which is not robust against node or link failures. Considering characteristics of wireless sensor networks (unreliable wireless links, energy resources) a single-path routing strategy cannot meet the requirements of various applications. A multipath routing strategy is an obvious approach to overcome the shortcomings of a single-path routing strategy.

One of the first works on multipath routing for packet switching networks was done by [4, 5], which they called "dispersity routing". The goal of their work was to distribute the data over multiple paths rather than concentrating on single paths. Following the same basic idea, recently, a lot of work has been done applying multipath routing in WSNs. In [6], load balancing has been achieved using multipath directed diffusion. The protocol creates multiple disjoint or braided paths for distributing traffic along these paths. The protocol also considers reducing overhead in basic directed diffusion (interests, exploratory data packets) by probabilistically forwarding packets and setting up forwarding threshold parameters. It considers *minimum node energy along a path* and *length of the path* to select a path for routing data. By probabilistic decision, it first utilizes shorter paths with high energy and then switches to longer paths. The paper focuses on load balancing and achieving desired network capacity using several paths, although constructing multipaths will help in making communication more robust against failures. Also, in a multipath routing strategy, paths formed can be braided, i.e., they share nodes with other paths or can be node-disjoint. To setup node-disjoint paths, there is some overhead involved as a node along a currently reinforced path can respond negatively to reinforcement messages, which try to reinforce it for other paths. In Multipath routing, after multiple path selection, data can be transmitted either concurrently along these paths to provide even traffic distribution [6, 7] or using the best path for data transmission and keeping additional paths for fault tolerance purposes [8].

Also, multipath routing has been proposed to combat topological instability (e.g., link failures) due to nodal mobility and changes in the wireless environment [9]. The work in [10] aims to develop multiple node-disjoint paths for robust data delivery. It proposes a deployment strategy that provides robustness to both short and long term node failures in ad hoc networks.

Multipath routing has been employed to improve quality of service (QoS) by reducing delays [11]. An important issue associated with sensor networks is the reliability and security of data [12, 13]. One important use of multipath has been proposed in [12] where the authors have proposed a multipath routing algorithm which delivers messages from the source by maintaining data confidentiality. The algorithm shares a secret message, first by creating its multiple shares, and then by distributing the shares along multiple paths, such that, even if a fewer number of nodes are compromised, the secret message will be secure.

The work proposed in the present paper takes the approach of using high-quality single path for data transmission, as using multiple paths for data dissemination might not be a good idea due to unreliable wireless links and interference between nodes in a dense WSN environment. The main idea behind the proposed method is to provide path resilience (against node failures) along with load balancing by constructing multiple paths using cumulative residual energy. It also incorporates multipath discovery without any overhead, since this approach does not explicitly try to achieve disjoint multipaths.

III. METHODOLOGY AND DESCRIPTION OF STAGES

The proposed method of constructing routing paths using cumulative residual energy was applied on directed diffusion. Before implementing multipath routing in DD, we improved the basic DD by incorporating load-balancing. This was done by updating residual energy values of the nodes, network wide, periodically at a low-rate as well as at a high-rate and by reinforcing nodes based on their residual energy values. The main contribution of this work is to implement multipath routing to improve load-balancing and to minimize path failures so that the network lifetime can be extended.

While various definitions of network lifetime have been used in the literature [14], we decided to define "network lifetime" or the termination of the simulation when the first node fails (dies). This definition seems appropriate for load balancing algorithms, since an ideal load balancing would have all the nodes loose energy at the same rate, so that they all die at the same time.

A. Neighbor Discovery and Interest Propagation

At the beginning, the network enters the neighbor discovery phase, in which each node tries to register its one-hop neighbors within its radio range. After this phase, each node has a *Neighbor_List* in its memory which is used for interest propagation. An 'Interest' is a query by the operator which can be diffused into the network at any node. This

 ISBN: 978-1-61208-231-8

node which initializes interest propagation is called the 'sink'. The sink broadcasts the interest message with its desired event type towards its neighbors. Whenever a node receives an interest message (not received previously from the sending node), it makes a new entry in its 'Interest_Table' along with a gradient for that interest. Each interest in the interest table has an associated '*Gradient_List'*, having IDs of nodes which sent the same interest to the current node. The gradient list is used to selectively route back exploratory data packets towards the sink. Interest message also has an 'interval' field, which specifies the data rate for the next event. The proposed method unlike many extensions to DD does not try to reduce overhead (by suppressing interest propagation setting up thresholds) as it maintains original characteristics of DD.

B. Exploratory Data and Energy Updates

Eventually the interest message will reach a node which can serve the sensing task specified in the interest message and this node is called the 'source' node, which will initiate exploratory data (ED) sending process periodically. The period of sending exploratory data is extracted from the interest message. ED is then forwarded from the source towards the sink using established gradients through multiple paths. Exploratory data packets (EDPs) are sent out periodically by the source at a lower frequency compared to interest message propagation. To incorporate load-balancing, this method allows each node to have information about the residual energy values of its neighbors and updates it periodically during each ED propagation phase. This is simply done by piggybacking (including) the residual energy value of the sending node on to its ED packet which is sent out to nodes on its gradient list. When this ED packet is received by a node, it will extract the energy update about the sender, and will store it in its *'Senders_List'* along with its residual energy value. In the basic directed diffusion, only the timestamps of ED senders are recorded and updated. After the ED phase, nodes will be having complete residual energy information about their neighboring nodes.

C. Multipath Discovery using Reinforcements

The proposed method reinforces two best paths at every Reinforcement phase for each interest. The sink initiates the Reinforcement phase after it has complete information about the residual energy values of its neighboring nodes. Sink sends out Reinforcement message packets (RMPs) to two of its nodes having highest residual energy. Reinforcing nodes based on residual energy introduces load-balancing in the network. Each node has an '*RMP_List'* which stores the *rmp_ID, hop_Count, CRE* values for each sender sending an RMP.

The two paths formed in our case can be braided i.e., they can be have common nodes along these paths. We do not use disjoint multipath formation due to overhead involved. The reason for reinforcing two paths is just the energy overhead involved with several paths. As RMPs propagate along reinforced paths, each node appends its residual energy value to the CRE field of an RMP. Eventually, these RMPs will find a source node which will then have information about each path's cumulative residual energy. This CRE for each path will specify the health of the path and source selects the one which has highest cumulative residual energy. By doing this, we can avoid bad paths which can fail any time. Also during RMP propagation, each node adds to the '*hop_Count'* field which is used by the source for estimating energy consumed by the path and updating its CRE during data transmission in between two RMP intervals (described in the next section).

D. Reinforced Data Propagation

Once the source receives reinforcement message packet, it arranges for the reinforced data packet (RDP) to be sent back at a higher rate towards the sink. Source in its RMP_List has information about each path's CRE and number of hops taken (hop_Count). CRE is given by (1):

$$CRE = \sum_{i=1}^{n} R_i \tag{1}$$

The R_i is the node *i's* residual energy along the reinforced path. The source node will select the path with the highest CRE and will forward the reinforced data packet (RDP) using this path. The proposed method piggybacks the residual energy value of the sender node onto the RD packet. This value is extracted by the node receiving the RDP and it will update its Senders_List with this residual energy value for the sender node. In this way, residual energy values are updated across the network at a higher rate compared to slower ED updates. Since the source node does not get any update about the CRE (before the next reinforcement) of the selected path while it's transmitting data through it, it estimates the CRE value of the path in use by simply using the hop count along that path and the energy consumed for transmission. While sending data along a chosen path the source node estimates the CRE using:

$$CRE = CRE - (hop\_Count * tx\_Energy) \tag{2}$$

In case, if source node finds the second path higher in CRE than the one being used, it will route data through this alternate path. By doing this the source can insure that it selects a healthy path every time for data transmission and can switch to another path dynamically if it finds degradation along the used path. With different paths being formed every time during the reinforcement phase and by utilizing the path high in energy resources, the proposed method provides load-balancing along with fault tolerance.

IV. EXPERIMENTAL RESULTS

A Java simulator was developed to simulate the effectiveness of the proposed cumulative residual energy (CRE) for creating multiple paths in directed diffusion. A Java simulator was chosen to enable comparison of the results of this work with previous work done by the authors [3]. Our next step will be to port the preliminary Java-based

 ISBN: 978-1-61208-231-8

simulations to ns2 for validation and comparison with other work in the field. This will be followed by applying the CRE method to real sensor nodes.

The three variants are referred to as: "Basic DD", "Load balanced DD with ED & RD energy-piggyback" and "Multipath DD with CRE piggyback". The network was simulated for different number of nodes from N=300, 400, ..., 600. Initial residual energy for each node was equal to $2x10^4$ Joules; radio range = 4 m. The energy consumption by a transmitting node was set to 2 J and 1 J for a receiving node, establishing a ratio of 2:1, as was done in [15]. In the simulations of the proposed CRE method, the ratio of transmission to reception energy consumption was not significantly sensitive to the exact ratio. For instance, the ratio was changed to 1.5:1, and it was found that the net effect on results was almost identical. The event triggering times for interests, exploratory data, reinforcements and reinforced data were 5 s, 10 s, 15 s and 1s respectively.

A. *Residual Energy Variance*

As we can see from Fig. 1, the proposed method has a lower variance (38%, 30%) in residual energy than that of the basic DD and load balanced DD respectively. By reinforcing paths based on high residual energy, instead of least-delay, and updating residual energy values at a higher opportunistic rate we can improve the energy variance of the basic directed diffusion, as shown by the result of "Load balanced DD with ED & RD energy-piggyback". However, by using the multipath DD scheme with proposed CRE based route construction we can see a significant improvement in terms of energy variance as well as network lifetime. This is because of the fact that the proposed method "Multipath DD with CRE piggyback" not only has the load-balancing capability which is implemented in a similar way to "Load balanced DD with ED & RD energy-piggyback" scheme but it also has source selective routing in which source tries to identify the high-quality path every time it send reinforced data. By switching traffic across different paths which are discovered every reinforcement phase, the network achieves more load-balancing than the previous improvement along with a measure to minimize node failures.

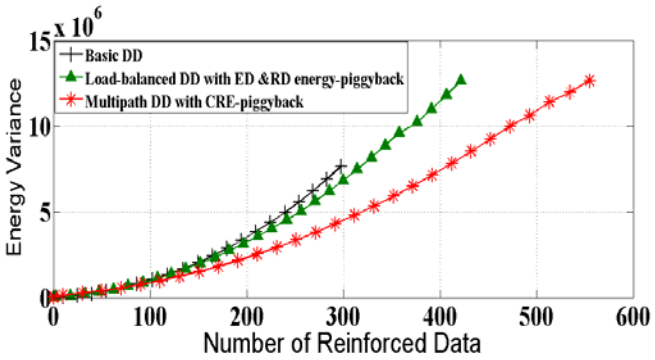


Figure 1. Variance of residual energy vs. average number of reinforced data events generated within the network (for 600 nodes).

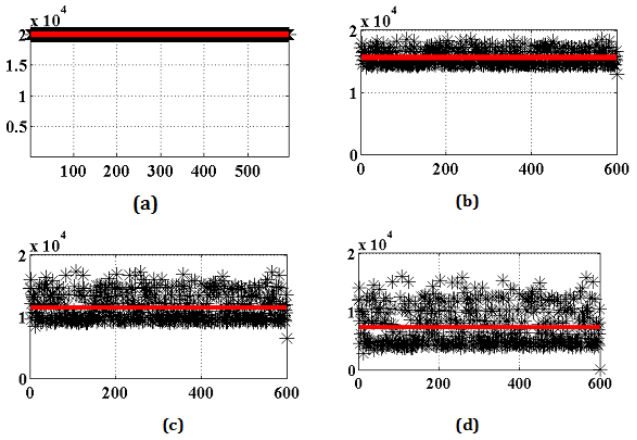


Figure 2. Residual energy and mean residual energy presentation of each node for the basic directed diffusion (four phases of network life).

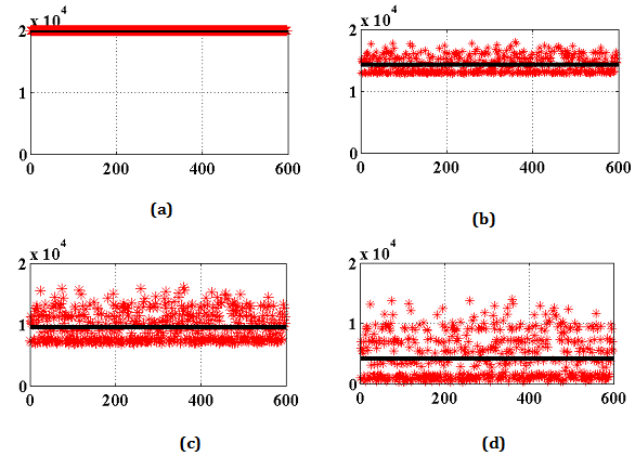


Figure 3. Residual energy and mean residual energy presentation of each node for the Multipath DD with CRE-piggyback (four phases of network life).

B. *Load Balancing*

In four phases of network life, the network's residual energy distribution for each node is plotted (before any one node died) for both cases of DD and the proposed multipath DD. Figures 1 and 2 compares the two schemes for 600 nodes. By comparing Fig. 2d (basic DD) with Fig. 3d (proposed method), it is clear that the proposed method was able to live longer by constructing quality paths using CRE, judiciously choosing nodes based on their residual energy and by gracefully lowering the average variance of residual energy near the "death floor" much better than basic DD.

C. *Network Lifetime*

In Fig. 4, we plot node density versus the number of reinforced data that were passed before any one node in the network died (R_i = 0). It is clear from the figure that the proposed method delivers more RD packets than the basic directed diffusion. The proposed method has a longer

 ISBN: 978-1-61208-231-8

network lifetime (85 %, 32%) than the basic directed diffusion and load-balanced directed diffusion respectively.

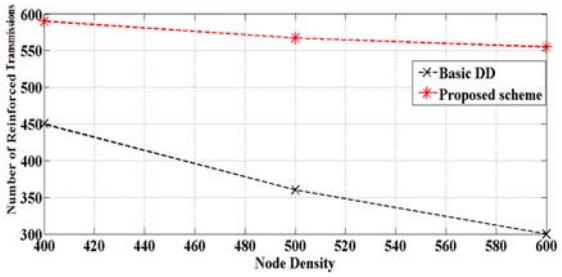


Figure 4. Average number of reinforced data generated within the network vs. number of nodes.

D. Operation

Fig. 5 illustrates the operation of the two main stages (reinforcement and reinforced data propagation) of the CRE method of constructing multiple paths. The Sink node reinforces two nodes with highest residual energy (node X and node Y), which, in turn, will reinforce those upstream nodes having the highest residual energy for any one reinforcement round. Each node along the paths thus formed includes its residual energy when reinforcing its upstream neighbor, and, thus, the cumulative residual energy readings accumulate along the paths. Eventually, the RMPs propagate through two paths and find the Source node. The source node (node Z) will determine the path with the highest cumulative residual energy (CRE1=24800 J), and will select that path for transmitting reinforced data for that reinforcement round. Reinforced data is sent along the selected path till the new reinforcement phase and the CRE value in the source is dynamically updated using (2).

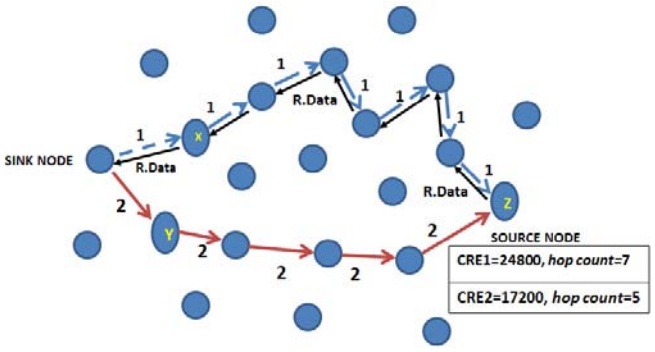


Figure 5. Illustration of the proposed CRE method. The Reinforcement and Reinforced Data propagation stages of the algorithms are shown.

V. Conclusion and Future Work

This paper presented an energy efficient method of load balancing and fault tolerance for wireless sensor networks. The proposed method constructs multiple paths using cumulative residual energy of the nodes along the path. The proposed method was added to and tested on the Load-balanced Directed Diffusion algorithm [3] to compare its performance. The simulation, analysis, and comparison with load-balanced Directed Diffusion and basic Directed Diffusion show that the proposed method has a lower variance in residual energy and a longer lifetime than both. The proposed method shows 30% improvement in residual energy at the time of network death and an average improvement of 32% in extending the lifetime of the network as compared with load-balanced Directed Diffusion. As compared with Directed Diffusion, the proposed method shows 38% improvement in residual energy at the time of network death and 85% improvement in extending the lifetime of the network.

Our future work includes evaluating multiple sinks and sources to verify its scalability. Also, by simulating the network with patterned failures we can testify its multipath advantage of recovery from bad paths.

A limitation (challenge) of the proposed CRE algorithm is that by considering only residual energy in the path establishment, this increased the latency and delay. The challenge here lies in optimizing the algorithm, so that it can balance between the latency and residual energy to construct optimized paths. Also, the simulation results (Fig. 3d) show that, although the network achieves a good load-balancing; there are still some nodes with high residual energy left, when the network dies. The challenge here is to utilize these nodes and improve load-balancing. Also, work is in progress to implement repair-mechanism to recover from disruptions caused by a node that goes down.

VI. References

[1] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless Sensor Network Survey”. Comput. Netw. , 52, pp. 2292–2330, 2008.

[2] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, “ Directed diffusion for wireless sensor networking,” IEEE/ACM Transactions on Networking, vol. 11, no. 1, pp. 2-16, Feb. 2003.

[3] S. Wijedasa, S. Rizvi, and K. Ferens, “Load balancing algorithms for wireless sensor networks”, Proc. The 2012 International Conference on Wireless Networks (ICWN'12), Las Vegas, Nevada, USA , pp. 61-67, 2012.

[4] N. F. Maxemchuk, “Dispersity routing in high speed networks”, Computer Networks and ISDN Systems, 25(6), pp. 645-661, 1993.

[5] N. F. Maxemchuk, “Dispersity routing on ATM networks”, IEEE INFOCOM’93, vol.1, pp.347-57, San Francisco, CA, Mar 1993.

[6] A. N. Eghbali and M. Dehgan, “Load-balancing using multi-path directed diffusion in wireless sensor networks”, Proc. of 3rd international conference on mobile ad-hoc and sensor networks, pp. 44-55, 2007.

[7] S. Li, R. K. Neelisetti, C. Liu, and A. Lim, “Efficient multi-path protocol for wireless sensor networks”, Int. Jr. of Wireless and Mobile Networks, vol. 2, No.1, pp. 110-130 , Feb. 2010.

[8] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, “Highly resilient energy efficient multipath routing in wireless sensor

 ISBN: 978-1-61208-231-8

networks", ACM mobile comput. and commun. Review, 5(4), pp. 11-25, Oct. 2001.

[9] A. Tsirigos and Z. J. Haas, "Multipath routing in the presence of frequent topological changes", IEEE Communication Magazine, 39(11),pp. 132-138, November 2001.

[10] Z. Ye, S. V. Krishnamurthy, and S. K. Tripathi, "A framework for reliable routing in mobile ad hoc networks", IEEE INFOCOM 2003, Sanfrancisco CA,vol. 1, pp. 270-280, Mar 2003.

[11] S. K. Das and A. Mukherjee, et al, "An adaptive framework for QoS routing through multiple paths in ad hoc wireless networks", J. Parallel Distributed Computing, 63(2003), pp. 141-153, 2003.

[12] W. Lou, W. Liu, and Y. Fang, "SPREAD: Enhancing data confidentiality in mobile ad hoc networks", IEEE INFOCOM 2004, Hong Kong, China, vol. 4, pp. 2404-2413, March 2004.

[13] W. Lou, Y. Zhang, W. Liu, and Y. Fang, "A multipath protocol for secure and reliable data collection in wireless sensor networks", technical report, ECE department, Worcester Polytechnic Institute, June 2004.

[14] Y. Chen and Q. Zhao, "On the lifetime of wireless sensor networks," IEEE Commun. Lett. , vol. 9, no. 11, pp. 976–978, Nov. 2005.

[15] E. Niewiadomska-Szynkiewicz, P. Kwaśniewski, and I. Windyga, "Comparative study of Wireless Sensor Networks energy- efficient topologies and power save protocols", Journal of Communications and Information Technology, vol. 3, pp. 68- 75, 2009.

 ISBN: 978-1-61208-231-8

Multi-dimensional Key Assignment for Hierarchical Media Access Control with Collusion Resilience

Shoko Imaizumi, Naokazu Aoki, and Hiroyuki Kobayashi
Division of Information Sciences
Graduate School of Advanced Integration Science
Chiba University
Chiba, Japan
Email: imaizumi@chiba-u.jp, aoki@faculty.chiba-u.jp, kobahiro@faculty.chiba-u.jp

Hitoshi Kiya
Dept. of Information and Communication Systems
Tokyo Metropolitan University
Tokyo, Japan
Email: kiya@sd.tmu.ac.jp

***Abstract*—We propose a multidimensional key assignment scheme using modified hash chains (MHCs) to hierarchically control access to scalable media. By introducing MHCs, the proposed scheme manages one key composed of a single key segment. The single managed key is not distributed to any user, providing security against key leakage. Collusion attacks caused by multiple users to obtain media with higher quality than that allowed by their access rights are prevented with the key assignment order. Our scheme also inhibits the growth of hash calculation. Performance analysis shows the validity of the proposed scheme.**

***Keywords-key assignment*; *access control*; *collusion attack*; *hash chain*; *cyclic shift*; *scalable media*.**

I. INTRODUCTION

With the growth in network technology, scalable transmission has become popular. Hierarchical access control to protect scalable media has been studied widely [1]–[8]. A simple and straightforward way to realize versatile access control for scalable media, to which several entities belong, is encrypting each entity individually. This approach, however, has to manage a large number of keys, given a large number of entities in a medium.

Hierarchical access control schemes have been proposed for scalable media [3]–[8], such as JPEG 2000 [9] coded images and/or MPEG-4 fine granularity scalability [10] coded videos, so that each user can obtain a medium at the permitted quality from one common enciphered codestream. OHCs (Ordinary hash chains) [11], hereafter, have also been introduced to several schemes for reduction of the number of key segments, which compose each key [5]–[7]. These OHC-based access control schemes increase the number of key segments, depending not only on the dimensions of scalability, but also on the hierarchical depth of scalability. Another scheme, which is also based on OHCs, has been proposed to reduce the number of key segments to one, but this scheme assumes the controlled media has only a single hierarchy [8].

In this paper, we propose an efficient key assignment scheme for hierarchical media access control. We assume that there is multi-dimensional scalability in each scalable medium. By introducing MHCs (modified hash chains), hereafter, the proposed scheme manages one key composed of a single key segment. The managed key is not distributed to any users, providing security against key leakage. Our scheme is also resilient to collusion attacks, in which malicious users illegally access media at higher quality than that allowed by their access rights. Moreover this scheme inhibits increasing the amount of hash calculation by using cyclic shifts.

This paper is organized as follows. Section II briefly describes hierarchical access control and mentions three requirements for hierarchical access control of scalable media. The new scheme is proposed in Section III, and is analyzed in Section IV. Finally, conclusions are drawn in Section V.

II. PRELIMINARIES

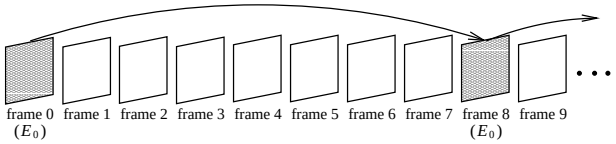
We briefly describe hierarchical access control for scalable media, and also summarize three requirements on key assignment for hierarchical access control, introducing some conventional schemes [5]–[7] to clarify the aim of this work.

A. Hierarchical Access Control

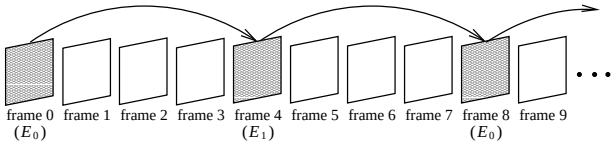
Firstly, we assume that scalable medium X has one-dimensional scalability ($J = 1$) and the scalability is frame rate, of which the hierarchical depth is $D_1 = 4$. As shown in Fig. 1, medium X should be decoded at 15 (Q_0), 30 (Q_1), 60 (Q_2), or 120 (Q_3) frames per second (fps). Fig. 2 shows a practical diagram of medium X. L_{d_1} $(d_1 = 0, 1, 2, 3)$ represents a set of frames decoded at 15, 30, 60, or 120 fps. Entity E_3 is a complementary set of L_2, that is frames decoded at 120 fps only. Similarly, E_2 and E_1 represent complementary sets of L_1 and L_0, respectively. E_0 represents the same as L_0, that is a set of frames decoded at each frame rate.

For another example, we also assume that scalable medium X has two-dimensional scalability ($J = 2$). One

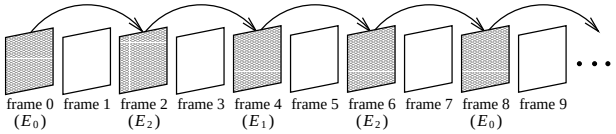
 ISBN: 978-1-61208-231-8



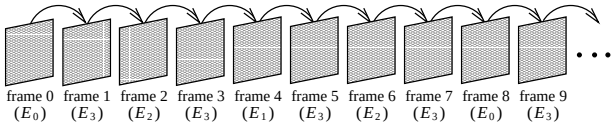
(a) 15 fps (Q_0).



(b) 30 fps (Q_1).



(c) 60 fps (Q_2).



(d) 120 fps (Q_3).

Figure 1. Hierarchical decoding of one-dimensional scalable medium X at frame rate Q_{d_1} ($J = 1$ and $D_1 = 4$ ($d_1 = 0, 1, 2, 3$)).

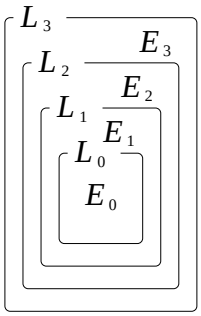
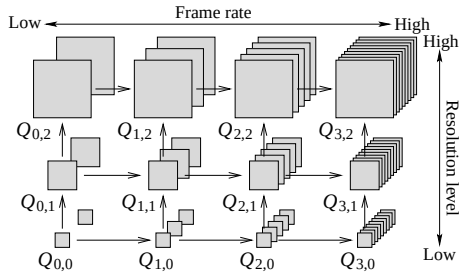
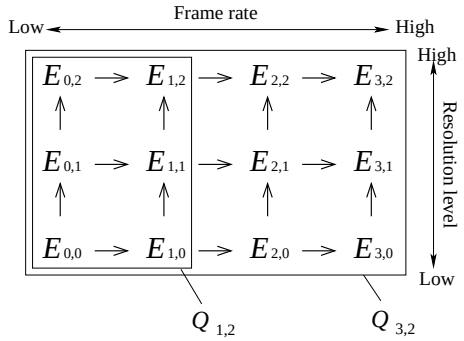


Figure 2. Practical diagram of medium X.

of the dimensions is frame rate and the other is resolution level, and the hierarchical depths of them are $D_1 = 4$ and $D_2 = 3$. Fig. 3 outlines an example of scalable decoding in which the scalable media with two-dimensional scalability ($D_1 = 4$ and $D_2 = 3$) are decompressed at different quality. The highest quality is $Q_{3,2}$. Medium X with quality $Q_{3,2}$ is obtained by decompressing all entities. To decode medium X at $Q_{1,2}$, six entities $E_{1,2}$, $E_{1,1}$, $E_{1,0}$, $E_{0,2}$, $E_{0,1}$, and $E_{0,0}$ are decompressed. Thus, access control for scalable media should encipher the codestream entity-by-entity using different keys.



(a) Decoding quality Q_{d_1,d_2}.



(b) Decoding order of entity E_{d_1,d_2}.

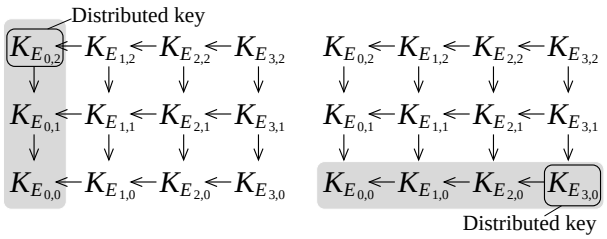
Figure 3. Hierarchical decoding of two-dimensional scalable medium X at frame rate and resolution level Q_{d_1,d_2} ($J = 2$, $D_1 = 4$ ($d_1 = 0, 1, 2, 3$), and $D_2 = 3$ ($d_2 = 0, 1, 2$)).

B. Requirements

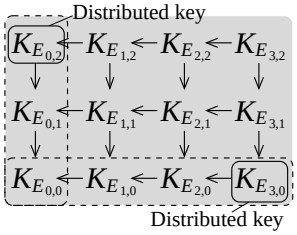
This section describes three requirements on key assignment for hierarchical access control of scalable media, i.e., collusion attack resilience, the less number of managed key segments, and the less amount of hash calculation.

1) Collusion Attack Resilience: Collusion attacks are caused by multiple users to obtain medium X with higher quality than that allowed by their access rights, and the conventional scheme [5], Scheme I hereafter, allows users to collude. The attacks are due to multiple key segments composing each key. In Fig. 4, the arrows indicate key assignment order. $K_{E_{d_1,d_2}}$ is a key for entity E_{d_1,d_2}, and $K_{E_{3,2}}$ is the initial key. As shown in Fig. 5, initial key $K_{E_{3,2}}$ is divided into two key segments $K_{1(3)}$ and $K_{2(2)}$. Each key segment is allocated to each dimension, and key segments $K_{1(d_1)}$ and $K_{2(d_2)}$ are derived from previous key segments $K_{1(d_1+1)}$ and $K_{2(d_2+1)}$, using OHCs [11]. By concatenating them, key $K_{E_{d_1,d_2}} = K_{1(d_1)} \parallel K_{2(d_2)}$ is derived.

In Fig. 4(a), Alice is allowed to access medium X at $Q_{0,2}$ and receives key $K_{E_{0,2}}$, which consists of two key segments $K_{1(0)}$ and $K_{2(2)}$. She can derive keys $K_{E_{0,1}}$ and $K_{E_{0,0}}$ and decipher $E_{0,2}$, $E_{0,1}$, and $E_{0,0}$. Whereas, Bob, in Fig. 4(b), receives $K_{E_{3,0}}$, consisting of $K_{1(3)}$ and $K_{2(0)}$, and derives $K_{E_{2,0}}$, $K_{E_{1,0}}$, and $K_{E_{0,0}}$ to decipher $E_{3,0}$, $E_{2,0}$, $E_{1,0}$, and $E_{0,0}$ for access to medium X at $Q_{3,0}$. In this scheme, they are possible to illegally derive $K_{E_{3,2}}$ by sharing $K_{1(3)}$ and



(a) Keys obtained by Alice. (b) Keys obtained by Bob.



(c) Keys obtained by their collusion attack.

Figure 4. Alice and Bob's collusion attack in the vulnerable scheme [5] (the shaded keys are obtained).

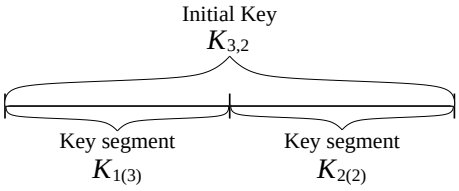


Figure 5. Initial key consisting of two key segments [5].

$K_{2(2)}$ with each other, so they can decipher all entities as shown in Fig. 4(c) and access medium X at $Q_{3,2}$. The proposed scheme is resistant to collusion attacks.

2) The Less Number of Key segments: Key assignment schemes that manage one key consisting of multiple key segments and subordinately derive other keys from the managed key have been proposed [5]–[7]. In these schemes, a key consists of multiple key segments.

First, Scheme I [5], which is vulnerable to collusion attacks, needs the same number of key segments as the number of the dimensions of scalability, J. The number of key segments in Scheme I, S_{I}, is

$$S_{\mathrm{I}} = J. \tag{1}$$

The second and third schemes [6], [7], Scheme II and Scheme III hereafter, control access to scalable media with collusion attack resilience. The number of key segments in Schemes II and III, S_{II} and S_{III}, are

$$S_{\mathrm{II}} = \prod_{j=2}^{J} D_j, \quad D_1 \geq D_2 \geq \cdots \geq D_J, \tag{2}$$

$$S_{\mathrm{III}} \leq \prod_{j=2}^{J} D_j, \quad D_1 \geq D_2 \geq \cdots \geq D_J, \tag{3}$$

respectively, whereas the proposed scheme needs a single key segment.

3) The Less Amount of Hash Calculation: To decrease the number of key segments, a cryptographic one-way hash function is introduced in Schemes I, II, and III. The maximum amount of hash calculation in these schemes, C_{I}, C_{II}, and C_{III}, are

$$C_{\mathrm{I}} = \sum_{j=1}^{J} \left(D_j - 1 \right), \tag{4}$$

$$C_{\mathrm{II}} = \prod_{j=1}^{J} D_j - 1, \tag{5}$$

$$C_{\mathrm{III}} = \prod_{j=1}^{J} D_j, \tag{6}$$

respectively. Thus, these amounts of hash calculation must increase, deepened the hierarchical depth of scalability, D_j. The proposed scheme is designed not to increase hash calculation substantially.

III. Proposed scheme

In this section, we propose a new key assignment scheme for access control of scalable media that manages one key consisting of a single key segment. The proposed scheme is resilient to collusion attacks the same as Schemes II and III, and does not increase the amount of hash calculation.

A. Key Assignment and Encipherment

As an example of scalable media for explanation, we assume three-dimensional scalable medium X ($J = 3$) shown in Fig. 6, where it is composed of four kinds of frame rates ($D_1 = 4$), three resolution levels ($D_2 = 3$), and two layers ($D_3 = 2$). Fig. 7 shows our proposed key assignment order, where $K_{E_{d_1,d_2,d_3}}$ is the key for entity E_{d_1,d_2,d_3} and K_m is the managed key. This order is resilient to collusion attacks. It is noted that a key is not composed of multiple key segments and consists of a single key segment in the proposed scheme.

Firstly key $K_{E_{3,2,1}}$ is derived from K_m as

$$K_{E_{3,2,1}} = h\left(K_m\right), \tag{7}$$

where $h(\cdot)$ is a cryptographic one-way hash function, i.e., the SHA-2 family (SHA-224, SHA-256, SHA 384, and SHA-512) [12]. Similarly, keys $K_{E_{d_1,d_2,d_3}}$'s are assigned on each of d_2 or d_3 ($d_2 = 2, 1, 0$ and $d_3 = 1, 0$) as

$$K_{E_{d_1,d_2,d_3}} = h^{3-d_1}\left(K_{E_{3,d_2,d_3}}\right), \quad d_1 = 2, 1, 0, \tag{8}$$

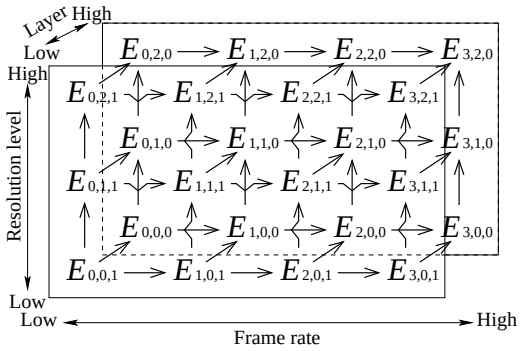


Figure 6. Decoding order of entity E_{d_1,d_2,d_3} in three-dimensional scalable medium X ($J = 3$, $D_1 = 4$, $D_2 = 3$, and $D_3 = 2$).

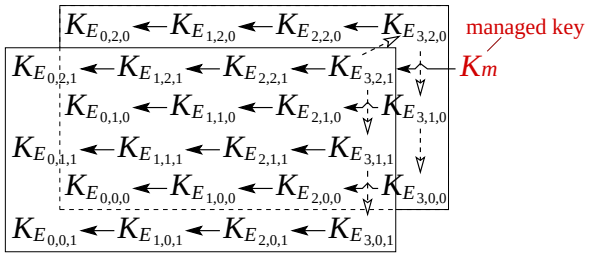
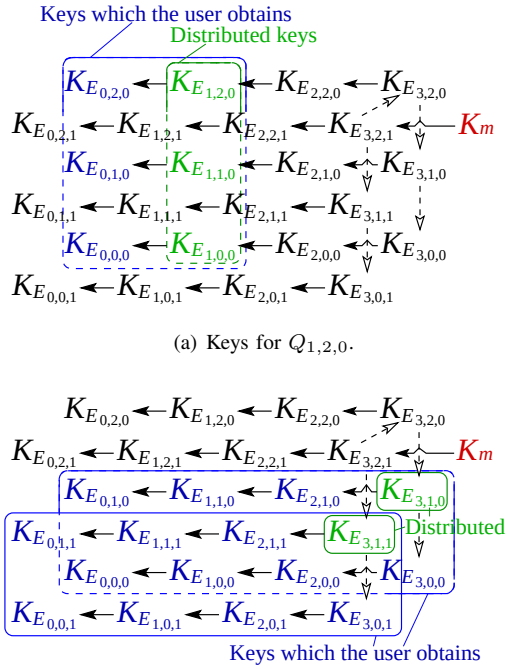


Figure 7. Key assignment to control access to three-dimensional scalable medium X shown in Fig. 6. Solid arrows are OHCs and dashed arrows represent MHCs.



(a) Keys for $Q_{1,2,0}$.

(b) Keys for $Q_{3,1,1}$.

Figure 8. Distributed and derived keys that the user needs to decompress medium X shown in Fig. 6 at certain quality.

respectively, where $h^{\alpha}(\beta)$ represents that $h(\cdot)$ is applied to β recursively α times. Keys $K_{E_{3,d_2,d_3}}$'s, except $K_{E_{3,2,1}}$, are given in the next paragraph. Eq. (8) represents OHCs [11], and the OHCs are shown with solid arrows in Fig. 7. Eq. (8) is also represented as

$$K_{E_{d_1,d_2,d_3}} = h\left(K_{E_{d_1+1,d_2,d_3}}\right), \quad d_1 = 2,1,0. \tag{9}$$

Meanwhile, keys $K_{E_{3,d_2,d_3}}$'s, except $K_{E_{3,2,1}}$, are assigned by MHCs. In this example, keys $K_{E_{3,1,d_3}}$, $K_{E_{3,0,d_3}}$ are given on each d_3 ($d_3 = 1,0$) as

$$K_{E_{3,d_2,d_3}} = h\left(s\left(K_{E_{3,d_2+1,d_3}}\right)\right), \quad d_2 = 1,0, \tag{10}$$

where $s(\cdot)$ is a cyclic shift. It is noted that the amount of each cyclic shift doesn't have to be secret information and that they can be opened to the public. Replacing the combination of $s(\cdot)$ and $h(\cdot)$ with $f(\cdot)$, which is an MHC, Eq. (10) is represented as

$$K_{E_{3,d_2,d_3}} = f\left(K_{E_{3,d_2+1,d_3}}\right), \quad d_2 = 1,0. \tag{11}$$

Key $K_{E_{3,2,0}}$ is also derived as

$$\begin{aligned} K_{E_{3,2,d_3}} &= h\left(s\left(K_{E_{3,2,d_3+1}}\right)\right) \\ &= f\left(K_{E_{3,2,d_3+1}}\right) \\ d_3 &= 0. \end{aligned} \tag{12}$$

It is noted that the amounts of cyclic shifts are secret information. The MHCs are shown with dashed arrows in Fig. 7.

By introducing MHCs, all keys $K_{E_{d_1,d_2,d_3}}$'s for all entities E_{d_1,d_2,d_3}'s are assigned based on managed key K_m. With key $K_{E_{d_1,d_2,d_3}}$, each entity E_{d_1,d_2,d_3} is enciphered. It is noted that any arbitrary symmetric encipher algorithm can be used in the proposed scheme.

B. Distributed keys and Decipherment

Here, it is considered that a user is allowed to access medium X with quality $Q_{1,2,0}$. The user receives keys $K_{E_{1,2,0}}$, $K_{E_{1,1,0}}$, and $K_{E_{1,0,0}}$ as shown in Fig. 8(a). To decompress medium X at $Q_{1,2,0}$, the user needs to decipher six entities $E_{1,2,0}$, $E_{1,1,0}$, $E_{1,0,0}$, $E_{0,2,0}$, $E_{0,1,0}$, and $E_{0,0,0}$. Three keys $K_{E_{0,2,0}}$, $K_{E_{0,1,0}}$, and $K_{E_{0,0,0}}$ are derived from distributed keys $K_{E_{1,2,0}}$, $K_{E_{1,1,0}}$, and $K_{E_{1,0,0}}$ as

$$K_{E_{0,d_2,0}} = h\left(K_{E_{1,d_2,0}}\right), \quad d_2 = 2,1,0. \tag{13}$$

By using six keys $K_{E_{1,2,0}}$, $K_{E_{1,1,0}}$, $K_{E_{1,0,0}}$, $K_{E_{0,2,0}}$, $K_{E_{0,1,0}}$, and $K_{E_{0,0,0}}$, corresponding entities are deciphered and decompressed to present medium X at $Q_{1,2,0}$.

As another example, we also assume that a user can access medium X with quality $Q_{3,1,1}$. The user receives two keys $K_{E_{3,1,1}}$ and $K_{E_{3,1,0}}$ as shown in Fig. 8(b). To access medium X at $Q_{3,1,1}$, the user has to obtain 16 of keys $K_{E_{d_1,d_2,d_3}}$'s ($d_1 = 3,2,1,0$, $d_2 = 1,0$, and $d_3 = 1,0$). $K_{E_{3,0,1}}$ and $K_{E_{3,0,0}}$ are derived from distributed keys $K_{E_{3,1,1}}$ and

 ISBN: 978-1-61208-231-8

Table I
COMPARISON WITH SCHEMES I [5], II [6], AND III [7]

Scheme	Collusion resilience	# Key segments	Max # hash calculation
Prop.	Yes	1	$\prod_{j=1}^{J} D_j - 1$
I [5]	No	J	$\sum_{j=1}^{J} (D_j - 1)$
II [6]	Yes	$\prod_{j=2}^{J} D_j$	$\prod_{j=1}^{J} D_j - 1$
III [7]	Yes	$\leq \prod_{j=2}^{J} D_j$	$\prod_{j=1}^{J} D_j$

$K_{E_{3,1,0}}$ using MHCs as

$$\begin{aligned} K_{E_{3,0,d_3}} &= h\left(s\left(K_{E_{3,1,d_3}}\right)\right) \\ &= f\left(K_{E_{3,1,d_3}}\right), \\ d_3 &= 1, 0. \end{aligned} \tag{14}$$

Then, 12 of keys $K_{E_{d_1,d_2,d_3}}$'s ($d_1 = 2, 1, 0$, $d_2 = 1, 0$, and $d_3 = 1, 0$) are assigned using OHCs as given in Eq. (8), and the user can decompress medium X at $Q_{3,1,1}$.

In the proposed scheme, the managed key is never distributed to any users in terms of security against key leakage.

IV. PERFORMANCE ANALYSIS AND COMPARISON

This section verifies that the proposed scheme meets requirements described in Section II-B. Table I shows the comparison result in terms of collusion attack resilience, the number of key segments and the amount of hash calculation, which are described in Section II-B. The proposed scheme is evaluated by comparing with three conventional schemes, i.e., Schemes I [5], II [6], and III [7], which use only OHCs.

A. Collusion Attack-Resistance

The proposed scheme is resilient to collusion attacks as well as Schemes II and III, while Scheme I is naive for the attacks.

In Fig. 6, we assume that Alice is allowed to access medium X at $Q_{0,2,0}$ and Bob is allowed to decompress it at $Q_{3,0,1}$. Alice receives three keys $K_{E_{0,n_2,0}}$'s ($n_2 = 2, 1, 0$). She cannot derive any keys from these distributed keys. In other hand, Bob receives two keys $K_{E_{3,0,1}}$ and $K_{E_{3,0,0}}$ and derives six keys $K_{E_{n_1,0,n_3}}$'s ($n_1 = 2, 1, 0$ and $n_3 = 1, 0$) using Eq. (8). They obtain ten valid keys in total, but they can not illegally derive any keys which they are not permitted to derive from these ten keys.

B. The Number of Key Segments

The proposed scheme manages one key consisting of a single key segment regardless of the dimensions of scalability and the hierarchical depth of scalability, while Schemes I, II, and III must manage multiple key segments, as given in Eqs. (1), (2), and (3).

The managed key is not distributed to any users in the proposed scheme in terms of security against key leakage, whereas the managed key segments are distributed to some users in Schemes I, II, and III.

C. The Amount of Hash Calculation

The maximum amount of hash calculation in the proposed scheme is $\prod_{j=1}^{J} D_j - 1$, which is the same as that in Scheme II, C_{II}, as given in Eq. (5). C_{III} is $\prod_{j=1}^{J} D_j$, as given in Eq. (6), and Scheme III must calculate once more than with the proposed scheme. Although C_{I} is less than those in other schemes, Scheme I is vulnerable for collusion attacks. It is noted that the proposed scheme needs cyclic shifts to assign some of keys.

V. CONCLUSION

This paper has proposed a novel key assignment scheme for hierarchical media access control, in which MHCs are employed. The proposed scheme can control access to scalable media with multi-dimensional scalability. The scheme manages one key composed of a single key segment. The single managed key is not distributed to any users. This scheme also prevents collusion attacks, in which malicious users illegally access media at higher quality than that allowed by their access rights. Performance analysis showed the effectiveness of our scheme. Future work will focus on applying this scheme to real systems.

ACKNOWLEDGMENT

This work was supported by JSPS KAKENHI Grant Number 23800010.

REFERENCES

[1] D. Xie and C.-C.J. Kuo, "Multimedia data encryption via random rotation in partitioned bit streams," in *Proc. IEEE ISCAS 2005*, pp. 5533–5536, 2005.

[2] Z. Zhang, Q. Sun, W.-C. Wong, J. Apostolopoulos, and S. Wee, "Rate-distortion-authentication optimized streaming of authenticated video," *IEEE Trans. Circuits Syst. for Video Technol.*, vol.17, pp. 544–557, May 2007.

[3] R. Grosbois, P. Gerbelot, and T. Ebrahimi, "Authentication and access control in the JPEG 2000 compressed domain," in *Proc. SPIE 46th Annual Meeting, Applications of Digital Image Processing XXIV*, vol.4472, pp. 95–104, 2001.

[4] Z. Shahid, M. Chaumont, and W. Puech, "Selective and scalable encryption of enhancement layers for dyadic scalable H.264/AVC by scrambling of scan patterns," in *Proc. IEEE ICIP 2009*, pp. 1273–1276, 2009.

[5] M. Joye and S. M. Yen, "one-way cross-trees and their applications," in *Proc. IACR PKC 2002*, pp. 355–358, 2002.

[6] S. Imaizumi, M. Fujiyoshi, and H. Kiya, "Efficient collusion attack-free access control for multidimensionally hierarchical scalability content," in *Proc. IEEE ISCAS 2009*, pp. 505–508, 2009.

[7] X. Zhu and C. W. Chen, "A collusion resilient key management scheme for multi-dimensional scalable media access control," in *Proc. IEEE ICIP 2011*, pp. 2825–2828, 2011.

 ISBN: 978-1-61208-231-8

[8] S. Imaizumi, M. Fujiyoshi, and H. Kiya, "An Efficient Access Control Scheme for Multimedia Content Using Modified Hash Chain," in *Proc. IARIA ICSNC 2011*, pp. 175–180, 2011.

[9] *Information technology — JPEG 2000 image coding system – Part 1: Core coding system*, ISO/IEC 15444–1, 2004.

[10] *Information technology — Coding of audio – Visual objects – Part 2: Visual*, ISO/IEC 14496–2, 2004.

[11] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM*, vol.24, no.11, pp. 770–772, 1981.

[12] NIST, *Secure Hash Standard*, FIPS PUB 180–4, 2012.

 ISBN: 978-1-61208-231-8

Group Key Establishment Scheme Using Wireless Channel Status

Seon Yeob Baek and Jongwook Park
The Attached Institute of Electronics and Telecommunications Research Institute (ETRI),
P.O.Box #1, Yuseong-gu, Daejeon, 305-600, Korea
E-mail: sybaek@ensec.re.kr and khspjw@hotmail.com

***Abstract*—Broadcast-based wireless communication is vulnerable to sniffing and eavesdropping by adversaries. Hence, wireless network security mechanisms have relied on cryptographic algorithms to protect information and support confidentiality. We propose a group key establishment scheme for secure wireless multicast services without a key management center. The proposed scheme exploits wireless channel reciprocity and generates an identical secret key among group users by steering pilot phase. We analyze and evaluate performance of the proposed scheme. Our results give an insight to determine transmit power strength and phase quantization-level according to the number of group users and group key size.**

***Index Terms*—Group key generation;group key establishment;secret key generation;secret key establishment;physical layer security**

I. Introduction

Security is a critical issue in wireless communication applications. Naturally, the wireless communication is based on broadcast of signal. Hence, if the signal is not encrypted, malicious adversaries can eavesdrop on the wireless communication and acquire the secret information from wireless sniffing. Most wireless network security mechanisms have relied on cryptographic algorithms to protect information and support confidentiality. The cryptographic algorithms require secret key establishment between users in a secure fashion. Key establishment consists of key generation and agreement. Secret keys are typically generated by the random number generator. Famous key agreement solution is Diffie-Hellman (D-H) algorithm [1]. The D-H algorithm is aimed at deriving symmetric keys over a unsecure channels. However, the D-H algorithm requires fast exponentiation and this is a cumbersome operation for mobile devices. Meanwhile, a key management center has been proposed to generate secret key and distribute the secret key securely. However, availability of the key management center is no longer guaranteed in ad-hoc networks. Therefore, key establishment has become more challenging in infrastructureless wireless networks [2].

There is increasing interest in utilizing wireless characteristics to improve wireless security [3]. The underlying wireless channel response between two users is unique, decorrelated rapidly in space, and dynamic in time. Hence, the wireless communication systems can utilize these characteristics to meet security requirements. The unique and decorrelated wireless characteristics can substitute traditional authentication protocols as a physical layer fingerprint [4]–[7]. Moreover, the dynamic and decorrelated wireless characteristics can provide randomness and uniqueness of secret key. Since eavesdroppers cannot infer the wireless channel response between two users, the wireless channel response becomes a basis to create common secret key in wireless networks [8]–[11]. Wireless channel reciprocity also supports simplified and secure secret key agreement scheme with time division duplex (TDD) mode. Since the wireless channel response of pilot signal has been already utilized for equalization or adaptive modulation and coding (AMC) scheme, wireless channel characteristic-based security schemes does not request additional radio resources for applications.

A variety of secret key establishment schemes based on radio channel reciprocity have been proposed to exploit various channel characteristics. Kai and Yunchuan have proposed the received signal strength (RSS)-based key establishment scheme using multiple antennas and adaptive channel probing, respectively [8], [9]. Suhas *et al* have proposed the level crossing-based key establishment scheme [10]. The RSS-based schemes have difficulty on quantization-level decision to acquire uniformly random sequence. On the other hand, the level crossing-based scheme needs guard area to reduce signal variation sensitivity. Qian *et al* have proposed a random phase-based pairwise and group key establishment scheme [11]. The phase-based key establishment scheme can achieve uniformly random key sequence and is controllable by a transmitter.

Previous wireless channel characteristic-based key establishment schemes have focused on peer-to-peer secret key. However, multiple users should share the common secret key for secure wireless multicast services. Qian *et al* have studied the wireless channel characteristic-based group key establishment scheme utilizing phase of the received signal [11]. Group users rotate pilot transmission and reception in multiple frames. Since duration time for key establishment is proportional to the number of users, the channel reciprocity might not be guaranteed in multiple frames for a large number of users. Key agreement probability (KAP) also decreases due to propagation of phase estimation error. Hence, we propose a novel group key establishment scheme for the secure wireless multicast services. The proposed scheme exploits wireless channel reciprocity and generates group key adjusting pilot phase only in a frame. To start group key establishment, group users select one master who can control pilot signal among them and others becomes clients. The master determines

 ISBN: 978-1-61208-231-8

TABLE I
NOTATIONS

Parameter	Definition
h_i	Channel gain of user i
M	Group key size
L	Number of group users
q	Quantization level
T	Frame duration
P_{sa}^{G}	Successful group SAP
θ	Phase of channel response
$\tilde{\theta}$	Estimated phase
κ	Group key
$h(\kappa)$	Hash value of group key

phase offset of clients and transmits phase-steered pilot signal according to each client's channel response. From the received pilot signal, clients can generate an identical group key.

The rest of this paper is organized as follows. In Section II, we propose a novel group key generation and agreement scheme based on phase steering. We analyze the proposed group key establishment scheme in Section III and evaluate performance of the proposed scheme according to the number of users and quantization level in Section IV. Finally, we present conclusion and future work in Section V.

II. GROUP KEY ESTABLISHMENT SCHEME

Multicast transmission is an efficient method when multiple users request identical information. In order to improve information security, multicast data should be encrypted by shared secret key among group users. However, it has been a tough issue to generate a group key and distribute the group key securely without a key management center. We propose a novel group key establishment scheme using wireless channel status.

Table I lists notations used in this paper and Fig. 1 shows wireless network environments for multicast transmission. There are six group users and two eavesdroppers. The eavesdroppers try to sniff data over the wireless channel. To start a novel group key establishment, group users select one master to generate group key among them and other users become clients. Wireless links, h_i, between master and each client i are independent of one another. The master transmits group key information hiding through wireless channel response. It is assumed the eavesdroppers have uncorrelated wireless channel with users. Hence, the eavesdroppers have no way of estimating channel response between the master and clients. The proposed key establishment scheme is scalable by relaying identical group key to other clients.

Fig. 2 shows one example of frame structure for the proposed group key establishment scheme. The selected master utilizes pilot resource of each client for fast key generation. The wireless communication system supports TDD mode. One frame consists of uplink and downlink modes. In uplink mode, clients transmit phase-fixed identical pilot signal to the mater. In downlink mode, the master transmits phase-controlled pilot signal to clients according to channel response of each client.

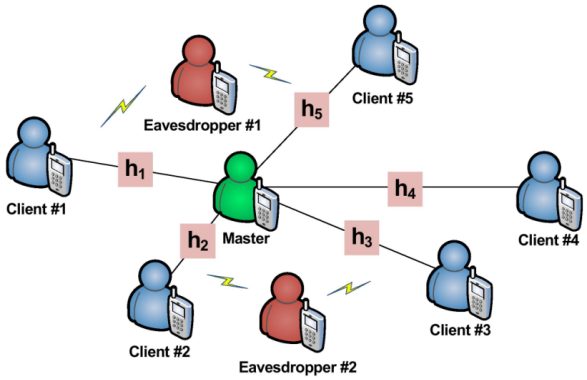


Fig. 1. Network Environment

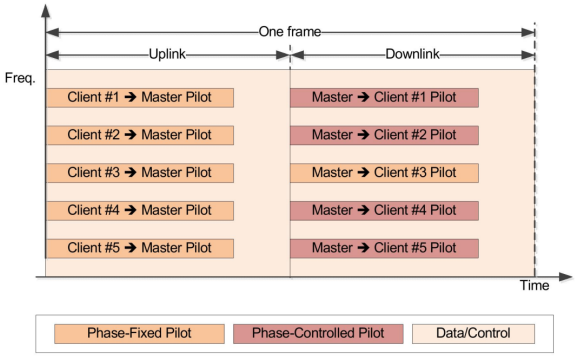


Fig. 2. Frame Structure

Since the pilot signal is controlled only during key generation period, phase-controlled pilot does not affect equalization or AMC scheme. Other resource except pilot signal is utilized to transmit data or control signal. It is assumed wireless channel response is quasi-static during key generation and thus users can exploit channel reciprocity.

Group key size and the number of users in a group is denoted as M bits and L, respectively. There are q symbols or quantization level. Hence, generated bits from one symbol is $\log_2 q$ bits. Successful symbol agreement probability (SAP) among group users and frame duration is denoted as P_{sa}^{G} and T, respectively. Then, expected group key generation time, $E[T_k]$, is proportional to

$$E[T_k] \propto \frac{M \cdot T}{\log_2 q \cdot P_{sa}^{G}}. \quad (1)$$

Fig. 3 describes the procedure of a proposed group key establishment scheme. The group key establishment scheme is divided into two steps as follows: group key generation and group key agreement between a master and clients.

In the first step, a client transmits a phase-fixed pilot signal, s_{12}, to a master. Then, the master estimates phase of the wireless channel response of the client, $\tilde{\theta}_{12}$. Meanwhile, there are candidate q pilot symbols to be transmitted by the master. These symbols are equally distanced for uniform randomness of the group key and each symbol represents unique binary sequence. The master selects one of candidate pilot symbols randomly and evaluate phase of the selected symbol, θ. The selected pilot symbol is applied identically to every client.

 ISBN: 978-1-61208-231-8

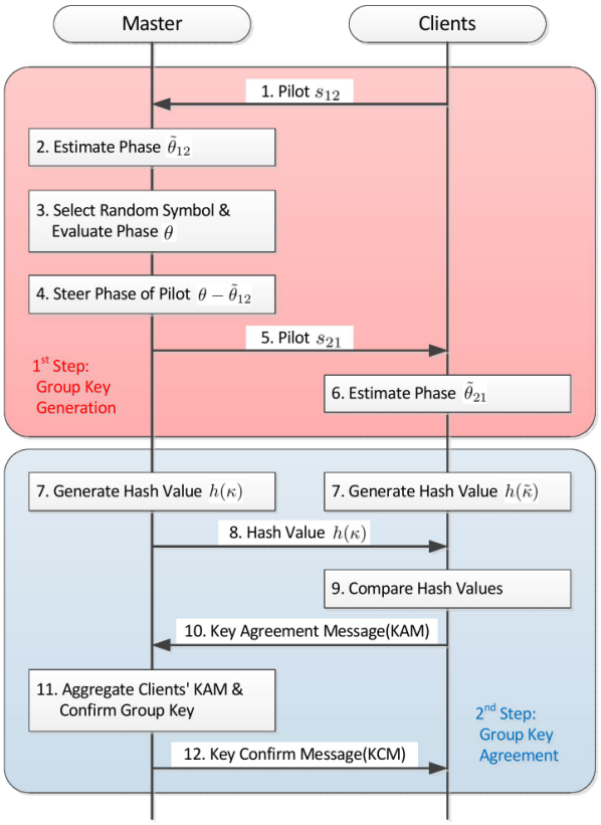


Fig. 3. Group Key Generation Procedure

From the selected symbol, the master compute phase offset, $\theta - \tilde{\theta}_{12}$. The master steers pilot phase according to the phase offset and transmits phase-steered pilot signal to the client. After pilot reception, the client estimates phase of the channel response, $\tilde{\theta}_{21}$ and extracts secret bits from $\tilde{\theta}_{21}$. The master and the client generate group key sequence aggregating secret bits from randomly selected symbol and estimated phase of the channel response, respectively. If the aggregated secret bit sizes are equal to the group key size, the master and the client finishes key generation and derives group key, κ and $\tilde{\kappa}$, respectively. Error correction code can be utilized for group key reconciliation.

In the second step, the master and the client generates hash value of the generated group key, κ and $\tilde{\kappa}$, respectively. Then, the master transmits hash value, $h(\kappa)$, to the client and the client compares the hash value with its own hash value, $h(\tilde{\kappa})$. Transmission of hash value can reduce data size to transmit and prevent sniffing. From comparison result, the client transmits key agreement message (KAM) that includes group key agreement information. The master aggregates KAMs received from multiple clients and confirms group key from KAMs. If every client has identical hash value with the master's hash value, the master transmits key confirm message (KCM) to clients. Otherwise, the master transmits key regeneration message (KRM) to clients and they restarts group key generation step.

To simply this procedure, an alternative scheme without KAM transmission is also possible. Every client transmits $h(\tilde{\kappa})$ to the master before the master transmits KAM. In this case, the master compares hash values received from clients and transmits KCM or KRM to clients. We can select one of two schemes adequately with regard to data size to be transmitted for key agreement.

III. Analysis of Group Key Establishment Scheme

We consider channel gain and noise at receiver for analysis model. Wireless channel gain has Rayleigh distribution and additive noise is zero-mean complex Gaussian random variables. From channel reciprocity, group users share the quasi-static wireless link. A master and a client experiences an identical channel gain but independent additive noise, respectively.

Pilot signal from the client to the master at time t is expressed as

$$s_{12}(t) = \exp[j(w_c(t - t_d))], \tag{2}$$

where w_c and t_d denotes carrier frequency and one-way link delay time, respectively.

Received signal at the master is expressed as

$$r_{12}(t) = h \cdot \exp[j(w_c t + \theta_{12})] + n_{12}, \tag{3}$$

where h, θ_{12}, and n_{12} denotes channel gain, shifted phase from channel response, and additive noise at the master, respectively. From the received signal (3), the master estimates phase of the channel response as $\tilde{\theta}_{12} = \theta_{12} + \theta^n_{12}$ due to the additive noise.

After pilot reception, the master selects one of candidate symbols randomly and evaluates phase, θ, from the selected symbol. Similar to M-ary Phase Shifting Keying (PSK), phases of candidate symbols are equally distanced and each phase denotes specific bit sequences such as Gray code. In order to derive an identical symbol, the master transmits controlled pilot signal according to the estimated phase offset, $\tilde{\theta}_{12}$, delay time, t_d, and normalized estimated channel gain, $|r_{12}|$. Hence, the pilot signal from the master to the client is expressed as

$$s_{21}(t) = \frac{\exp[j(w_c(t - t_d) + \theta - \tilde{\theta}_{12})]}{|r_{12}|}. \tag{4}$$

After the client receives pilot signal from the master, she or he recovers transmitted symbol and extracts secret key bits. The received signal at the client is expressed as

$$r_{21}(t) = \frac{h}{|r_{12}|} \cdot \exp[j(w_c t + \theta + \theta_{21} - \tilde{\theta}_{12})] + n_{21}. \tag{5}$$

The estimated phase at the client is denoted as $\tilde{\theta}_{21}$ and is equal to $\theta + \theta_{21} - \tilde{\theta}_{12} + \theta^n_{21}$. Since θ_{12} is identical to θ_{21}, $\tilde{\theta}_{21}$ is derived as $\theta + \theta^n_{21} - \theta^n_{12}$. The estimated phase error at the clients becomes $\theta^n_{21} - \theta^n_{12}$ and shows similar distribution with M-ary PSK transmission in Rayleigh channel [12]. Joint probability density function (PDF) of received signal vector r, and angle θ, is obtained as

$$p(r, \theta) = \frac{r}{\pi N_0} \exp\left\{ \frac{1}{N_0}(r^2 - 2\alpha\sqrt{2E_s} r \cos\theta + 2\alpha^2 E_s^2) \right\}, \tag{6}$$

 ISBN: 978-1-61208-231-8

where N_0 is noise variance, α is channel gain of the received signal, and E_s is symbol energy. Since we are interested only in the angle, we obtain the marginal pdf of angle as

$$p(\theta) = \int_0^\infty p(r,\theta)dr \quad (7)$$

$$= \frac{1}{\pi}\exp(-2\gamma\sin^2\theta) \times \int_0^\infty x\exp\left(x-\sqrt{2\gamma}\cos\theta\right)^2 dx, \quad (8)$$

where γ is the received symbol energy-to-noise ratio.

For q symbol-level quantization, symbol error probability (SEP) with Es/No value of γ is expressed as

$$P_q(\gamma) = 1 - \int_{-\pi/q}^{\pi/q} p(\theta)d\theta \quad (9)$$

$$\approx \sqrt{\frac{2}{\pi}}\int_{\sqrt{2\gamma}\sin\frac{\pi}{q}}^\infty \exp\left(-\frac{x^2}{2}\right)dx \quad (10)$$

$$= 2Q\left(\sqrt{2\gamma}\cdot\sin\frac{\pi}{q}\right), \quad (11)$$

where $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-\frac{u^2}{2}}du$.

The wireless channel gain follows Rayleigh distribution and is expressed as

$$p_\gamma(x) = \frac{1}{\gamma}\exp\left(-\frac{x}{\gamma}\right). \quad (12)$$

From (11) and (12), symbol agreement probability (SAP) of user i is expressed as

$$P_{sa}^i = \int_0^\infty P_q(x)p_\gamma(x)dx. \quad (13)$$

Finally, probability of successful SAP among L group users, P_{sa}^G, is derived as

$$P_{sa}^G = \prod_{i=1}^{L-1} P_{sa}^i. \quad (14)$$

IV. Performance Evaluation

We evaluate and compare the performance of the proposed group key establishment scheme with computer simulation results in this section.

Fig. 4 shows the SEP of the proposed scheme in Rayleigh channel. Solid lines and symbols represent the analytic and simulation results, respectively. The analytical results are quite analogous to the simulation results. Rayleigh channel gain, additive noise and quantization level affect the performance of SEP. As quantization level decreases or the value of Es/No increases, the performance of SEP is improved because Hamming weight between each symbol increases. To meet 1[%] of SEP, each quantization level of 2, 4, 8, 16 requires 15, 20, 25, 30[dB] of Es/No, respectively. This means approximately additional 5[dB] transmit signal strength enhancement is required to generate group key two times faster in Rayleigh channel environments. Fig. 5 shows the SEP of the proposed scheme without channel gain normalization. In this case, $|r_{12}(t)|$ in (4) is fixed to one. Therefore, the channel gain

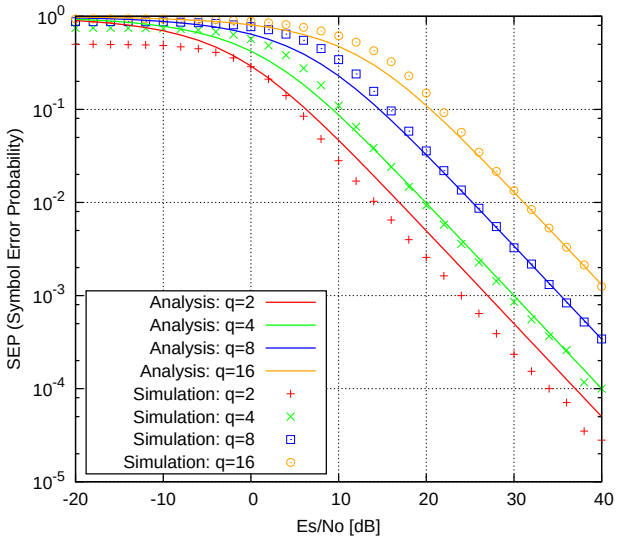


Fig. 4. Symbol error probability(SEP) of the proposed group key establishment scheme in Rayleigh channel

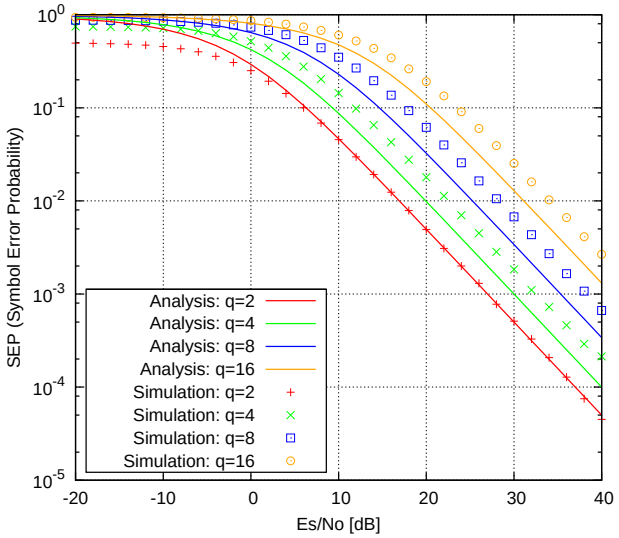


Fig. 5. Symbol error probability(SEP) of the proposed group key establishment scheme without channel response normalization in Rayleigh channel

affects the estimated phase severely and thus shows worse performance compared to the proposed scheme with channel gain normalization.

Fig. 6 shows the SAP of the proposed scheme for varying the number of group users. Each line and symbol represents quantization level and the number of group users except one master, respectively. As quantization level increases, the performance of SAP is worsened because Hamming weight between each symbol decreases. As the number of group users increases, high symbol energy is required to derive an identical key among group users. Every group user might have an identical key symbol approximately above 25[dB] of Es/No regime.

From (1), there is a tradeoff between quantization level, q,

 ISBN: 978-1-61208-231-8

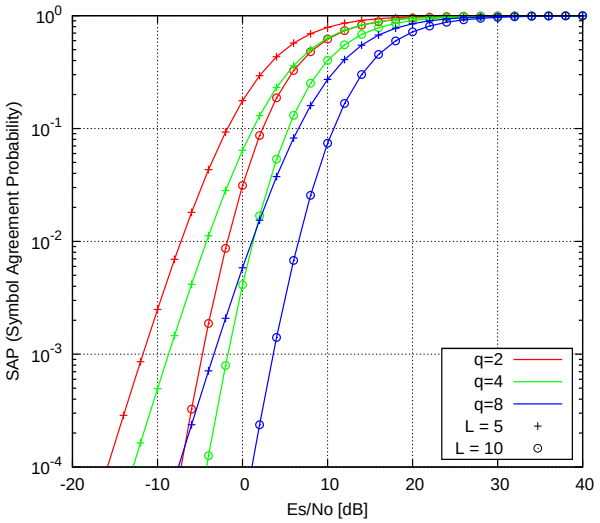


Fig. 6. Symbol agreement probability(SAP) of the proposed group key establishment scheme for varying the number of group users and quantization level in Rayleigh channel

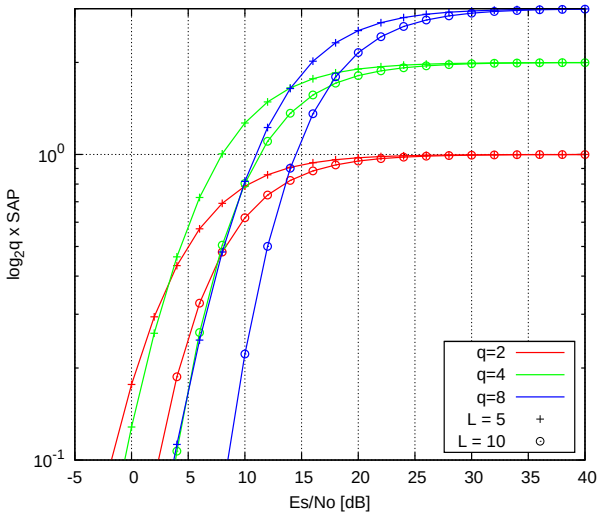


Fig. 7. Key generation rate of the proposed group key establishment scheme for varying the number of group users and quantization level in Rayleigh channel

TABLE II
THRESHOLD VALUES FOR QUANTIZATION LEVEL SELECTION

L	q	Threshold Values [dB]
5	2 ⇔ 4	3.3
5	4 ⇔ 8	13.9
10	2 ⇔ 4	7.7
10	4 ⇔ 8	17.6

and SAP, P_{sa}^{G}, to reduce group key establishment time. Higher quantization level generates more secret bits per a sample but results in degradation of SAP. Therefore, appropriate quantization level and transmit power strength is required to achieve fast group key establishment.

Fig. 7 shows key generation rate of the proposed group key establishment scheme for varying the number of group users. From Fig. 7, the threshold value of Es/No determine quantization level, q. For five group users, 3.3[dB] and 13.9[dB] of Es/No is the threshold value to transmit quantization level from 2 to 4 and 4 to 8, respectively. For ten group users, 7.7[dB] and 17.6[dB] of Es/No is the threshold value to transmit quantization level from 2 to 4 and 4 to 8, respectively. Table II lists threshold values for quantization level selection for varying the number of group users. As the number of group users increases, the required Es/No values also increases to utilize high order of quantization level.

V. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a phase-based group key establishment scheme using wireless channel status. With phase steering of the master, every group user can generate an identical group key without the key management center. Our analysis model evaluates performance of the proposed group key establishment scheme in terms of SEP and SAP for varying Es/No, the number of group users, and quantization-level. The evaluated performance of the proposed scheme gives an insight to determine transmit power strength and quantization-level according to the number of users and group key size. The proposed scheme can establish group key efficiently for wireless multicast services in infrastructureless networks. Our future work is to implement the proposed scheme and perform field test using SDR Platform.

REFERENCES

[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Information Theory*, vol. 22, no. 6, pp. 644-654. November 1976.
[2] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang and H.-H. Chen, "Physical Layer Security in Wireless Networks: A Tutorial," *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66-74. April 2011.
[3] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer,* Springer, 2009.
[4] J. Pang, B. Greenstein, R. Gummadi, S. Seshan, and D. Wetherall, "802.11 User Fingerprinting," in *Proc. of ACM MobiCom*, Montréal, Canada, September 2007, pp. 99-110.
[5] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," in *Proc. of ACM MobiCom*, San Francisco, USA, September 2008, pp. 116-127.
[6] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe,"Using the Physical Layer for Wireless Authentication in Time-variant Channels," *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2571-2579. July 2008.
[7] K. Zeng, K. Govindan, and P. Mohapatra, "Non-Cryptographic Authentication and Identification in Wireless Networks," *IEEE Wireless Communications*, vol. 17, no. 5, pp. 56-62. October 2010.
[8] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting Multiple-Antenna Diversity for Shared Secret Key Generation in Wireless Networks," in *Proc. of IEEE INFOCOM*, San Diego, USA, March 2010, pp. 1-9.
[9] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive Wireless Channel Probing for Shared Key Generation," in *Proc. IEEE INFOCOM*, Shanghai, China, April 2011, pp. 2165-2173.
[10] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel," in *Proc. of ACM MobiHoc*, San Francisco, USA, September 2008, pp. 128-139.
[11] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and Scalable Secret Key Generation Exploiting Channel Phase Randomness in Wireless Networks," in *Proc. of IEEE INFOCOM*, Shanghai, China, April 2011, pp. 1422-1430.
[12] J. Proakis, *Digital Communications,* Mc Graw Hill, 2000.

 ISBN: 978-1-61208-231-8

Design of IT Keys and Its Real Practice Specialist Program to Promote Key Engineers as Security Specialists

Atsuo Inomata, Satoshi Matsuura, Kenji Ohira, Youki Kadobayashi, Kazutoshi Fujikawa, Hideki Sunahara and Suguru Yamaguchi
Graduate School of Information Science
Nara Institute of Science and Technology
Ikoma-city, Nara-pref, Japan
e-mail: {atsuo, matsuura, k-ohira, youki-k, fujikawa, suna, suguru}@itc.naist.jp

***Abstract*—We introduce a practical teaching strategy called "IT Keys" for information security management. The educational goal is to put the work-ready graduates out into the social as a security expert (CSO: Chief Security Officer or CISO: Chief Information Security Officer). We collaborated with four universities and some departments of the Japanese government for IT Keys program. In this paper, we describe how to construct the teaching strategy, based on a combination of problem-based and project-based learning for promoting security expert. Furthermore, through the use of IT Keys for 5 years since 2008, we report evaluations of some special lectures and exercises according to every feedback each of year.**

Keywords-IT Keys; information security; education; problem-based learning; project-based learning; government.

I. INTRODUCTION

Information technology is an important and integral part of the current social infrastructure. Internet has come to play an important role in various foundations of our society and life. To maintain all our systems and ensure infrastructure safety, many organizations, government bodies, and companies employ security experts. In addition, they have engineers to carry out their work properly. However, very few people must have heard of a management technique or a policy for information security. Training these professionals is costly because their training involves imparting not only technical skills such as machine installation or specific procedures, but also special skills concerning law, policies, inspection, management, and ethics. These are necessary for taking decisions regarding the security policy of organizations, which is called the information security literacy. We believe that it is very important for future security experts to acquire and promote information security literacy more safely and reliably. Further, we believe that communities of students from different universities, organizations, and fields are important factors in the education for the information security.

In this paper, we propose a novel and practical teaching strategy called IT Keys that is a combination of problem-based and project-based learning. We particularly focus on "HORENSO" (in Japanese) [7], which is an information sharing technique based on members' understanding and synchronizing actions for changing circumstances within and outside an organization. The "HO" is the short form of "report," meaning timely and adequate reporting. Its flow is usually from subordinates to superiors. However, superiors or administrators must also ensure that subordinates are kept informed in order to ensure timely reporting. "REN" is "contact" and "SO" is "consult". This says that when a problem occurs, workers should report the issue, and not keep it to themselves. They should contact the relevant people, the foreman or the Japanese coordinator in this case. Instead of assuming that they can fix it themselves, they should consult with others to get their advice. Therefore, we believe that "HORENSO" is the most important factor for the information security experts to understand correctly.

In Japan, IPA [8] is an organization of professionals that contributes to the growth and advancement of Japan's economy by providing the strategic technology and human resource infrastructure required to support sustainable development of software and information processing systems. IPA provides a skill map of information security management to different categories of IT users. The map defines the security skill level in terms of a set of some technological elements. Further, it presents the quantification and visualization of the security skill required to grasp a level of each element. It can be considered as a measure that evaluates the level of competency required for information security management. Companies, organizations, and institutes can customize skill maps themselves according to their requirements. Skill maps can be classified into 16 classes on the basis of the type of technical skills to be acquired by information security professionals.

II. IT KEYS PROGRAM

IT Keys program (special IT program to promote key engineers as security specialists) was started in October 2008 as one of "IT Specialist Training Promotion Program" by the Ministry of Education, Culture, Sports, Science and

 ISBN: 978-1-61208-231-8

Technology (MEXT), Japan, for the promotion of the best standards in the field of information security. The purpose is to establish a strong and practical education foundation through industry-university cooperation to allow skilled people in the field of management of advanced and practical information security to interact. This is achieved by the cooperation of the teachers from four universities (NAIST, Kyoto University, Osaka University, JAIST) and working members of NTT Communications) and three organizations (NICT, JPCERT/CC, NPO-the Research Institute of Information Security). We aim lead to realize the following by training talented people in IT Keys.

Fig. 1 shows three fundamental keys for IT Keys knowledge acquisitions: (1) advanced knowledge, (2) practical knowledge, and (3) fundamental knowledge. In the case of acquisition of advanced knowledge, it focuses on comprehensive and rigorous social knowledge for information security, consisting of security policies, laws, security management, and ethical issues. In the case of acquisition of practical knowledge, it targets latest knowledge on information security, especially the cryptography theory, network security techniques, standardization of these techniques, network operation, etc. In the case of acquisition of fundamental knowledge, the study is based on basic computer science and mathematics knowledge in order to logically understand.

1. We make all learners study and understand not only the technology involved but also laws, policies, management techniques, and ethics with stress on systematic learning. We train about 20 people every year.

2. Through industry-university cooperation, we established a new educational foundation that helps in raising talented people who can take multifaceted information security countermeasure that a company or an organization needs.

3. We train students at a single center and make them study and exercise together closely. They can not only learn but also generate future human resource by forming human networks. So, we think that to get student together is a most important factor of IT Keys for them.

4. We realized social cognition by (1) conducting open lectures to present exercises and results to the public, (2) considering the results of an evaluation carried out by organizations for many kinds of IT business, (3) extending the cooperation of various external organizations, and (4) continuously improving the IT Keys program.

5. We contribute to the realization of an IT society in Japan, which will ensure the safety of all people, by reducing the social IT risk and establishing high-level information security through training security engineers and administrators and spreading awareness regarding information security among people.

III. HOW TO DESIGN

A. *Problem-based and Project-based learning on IT Keys*

We focused on the integration of problem- and project-based learning in IT Keys. Problem-based learning is conventionally restricted to classrooms. A group of learners (for example, 2 to 6 members) meet at a place where an instructor can facilitate a discussion on learning issues. Individual research may be conducted off-campus, but collaborative learning integral to this methodology is enabled by face-to-face communication and the process of negotiation of important learning issues. Savin-Baden introduced computer-mediated collaborative problem-based learning as a model that combines the current trend of online learning within universities, with problem-based learning focused on instructional methodology. Meanwhile, project-based learning is an instructional methodology adopted for the “Interactive design for multimedia” course that had a multiphase project as the major assessment component.

A combination delivery mode, for example, was used, and non-compulsory lectures were given and supplemented with practical sessions that involved support groups. This is based on a combination of problem- and project-based learning. Hence, we set up various problem scenarios in which a clear solution does not exist and then adopted both planning and learning to obtain a solution not by a single person but by cooperative work. IT Keys consist of the following 2 lectures and 5 exercises: information security management literacy, most recent information security issues, accident response exercise, risk management exercise, system attack and defense exercise, system break-in and analysis exercise, and IT crisis management exercise.

B. *Lecture on information security management literacy*

In a lecture on information security management literacy, some expert engineers gave information on the latest technologies to learners; for example, an engineer presented real raw traffic data and a case on an accident associated with an Internet service provider. This lecture was developed by an ISP engineer and manager, a lawyer, a government administrator (National Information Security Center, NISC), an auditing company, etc. This lecture provides a comprehensive and rigorous account of information security, consisting of topics on security policies, laws, security management, and ethical issues besides latest technologies. Thus, learners are also taught management techniques. According to hot security incidents on every year, we are updating the courseware, especially at

 ISBN: 978-1-61208-231-8

this year, we have added the digital forensics, cloud security and smartphone security.

C. Lecture on latest information security issues

In a lecture on latest information security issues, some professors presented theoretical and technical issues. The former deal with the basic algebra, fundamentals of public key infrastructure, and development of digital signature and elliptic curve cryptography [9]. Elliptic curve cryptography is the most attractive public key cryptosystem since it realizes the privacy protection with a small key size while maintaining the security high. This is why the elliptic curve is currently attracting a great deal of attention from a low power machine such as a smart card. Furthermore, a new tool from elliptic called a bilinear pairing, cast a new light on various problems on cryptology. In this lecture, we execute an exercise for implementing a bilinear pairing on Python language. Also the technical issues deal with basic network security mechanisms such as intrusion detection systems or development of firewalls. We provide some information systematically so that they can trouble shoot and take countermeasures against various accidents.

D. Exercise in IT crisis management

In the exercise called IT crisis management, learners work on a virtual ISP, and each group consists of 4 learners. They are responsible for the operation and management of web-hosting services for virtual customers. Further, they develop network equipment and some servers for this exercise in advance. Each group has an IP telephone, some routers and switches, network devices, PCs, etc. In practical situations, several security accidents can occur. The exercise staffs in backyard call and claim as various customers and then force their servers and services suspend or stop (Fig. 2). Each learner attempts to take countermeasures for unexpected accidents, to restore web-hosting services, deal with claims from customers, and find the reasons behind accidents. Finally, each group gives a clear and detailed explanation about the accidents and countermeasures to the CEO or President of ISP (Fig. 3).

E. Exercise in dealing with security incident

In the exercise called dealing with security accidents, learners work on a real security testbed called “StarBED” developed by National Institute of Information and Communications Technology (NICT).

Real computers and network equipment are required to evaluate the software practically for the Internet. In StarBED, there are many computers and switches, which connect these computers. We reproduce situations close to real situations using real equipment that are used on Internet. This idea is based on our previous work [5]. If developers want to evaluate their real implementation, they have to use real equipment. We believe that it is important for learners to emphasize on hands-on learning in real complicated Internet environments such as in the case of “StarBED” to monitor, analyze, and prevent Internet accidents and a variety of attacks and to deal with them. Another important factor is to learn more about computer viruses and malwares in order to understand the mechanism of cyber attacks. Fig. 4 shows snapshots of this exercise. We analyzed malware attacks (8 specimens) sampled from over 5000 e-mail viruses.

F. Exercise in risk management

In the exercise called risk management, learners learn the “internal behavior” of real malwares after the exercise on dealing with security accidents, which comprises learning the external behavior. Learners were studying at Telecom-ISAC Japan. The objective of Telecom-ISAC Japan is to enhance security countermeasures for the information and telecommunication industry, by establishing the systems for sharing between the members and analyzing the security accidents. Hence, it is important for them to study practical countermeasures against new malwares. Learners are responsible for analyzing and determining the internal behavior of malwares using analyzing tools. This also helps in taking the right action when a computer access accident comes to light. To recognize and respond to these situations, they learn about an analyzing technique at the machine language level (in this exercise, only Intel IA32 [10] Architecture) to detect suspicious codes or operations at the early stage. Fig. 5 shows snapshots of this exercise.

IV. EVALUATION

In order to verify the validity of the learning method for IT Keys, we carried out two evaluations. One was based on a questionnaire.

・Two or more traps were baited and devised in one incident scenario, it was very interesting for each other.

・For various situations and causes for an incident case which were occurred in this exercise, a communication to customer or a negotiation to group members simultaneously, these various experiences became future good tips.

・Since we could tackle some problems only by forming a small group and the exercise equipment and system was ready, we were able to play as each role for a virtual security division. However, since there were too many tasks to be completed in a short time, it was difficult and tough to complete unexpected incident.

Furthermore, we conducted a test based on the skill map, repeating the test 3 times from 2008 to 2011. This skill test was given twice to all learners, before and after the completion of the IT Keys courseware. For 2008, the average score in the first test was 52.7 and in the final test was 71.3; for 2011, the score in the first test was 55.7 and in the final test was 85.1 (out of 100). On 2008, we confirmed that the scores of tests on the topics “information security management,” “application security,” and “law, ordinance, and standard” had increased greatly. However, we found that the overall scores for “cryptography” and “law, ordinance, and standard” were low. In order to improve

 ISBN: 978-1-61208-231-8

comprehension, we implemented some feedbacks in the IT Keys courseware. For better understanding of the cryptography theory, we made learners use the Mathematica and Python language to implement a protocol for elliptic curves themselves. Then, we clarified the cryptography theory and its applications systematically. In addition, we subdivided the chapter on law, ordinance, and standard into 2 chapters and then evaluated their comprehension clearly from 2009. Consequently, the scores increased considerably. We found that the most important thing for educating a security expert is to keep on updating and feedback due to learner's level of understanding.

V. SUMMARY

We have conducted the special security expert education program supported by MEXT. From 2011, we continue it on our independent efforts. At March 2012, finally MEXT gave IT Keys a very good evaluation (most high degree) [6].

REFERENCES

[1] Slavin, R.E., Cooperative Learning: Theory, Research and Practice (2nd edition), Boston: Allyn and Bacon press, 1995.

[2] Savin-Baden M., Facilitating Problem-based Learning: Illuminating Perspectives, Open University Press, 2003.

[3] Savery, John R., "Overview of Problem-based Learning: Definitions and Distinctions", Interdisciplinary Journal of Problem-based Learning, Vol.1, Article 3, pp.9-20, 2006.

[4] Frank K.. and Michelle R., "Project-based learning and learning environment", Issues in Information Science and Information Technology press, Vol. 4, pp.503-510, 2007.

[5] Gregory Blanc, Youki Kadobayashi, "A step towards static script malware abstraction: Rewriting obfuscated script with Maude", IEICE Transactions on Information and Systems, Vol. E94-D, No.11, pp.2159-2166, 2011.

[6] MEXT, available at http://www.mext.go.jp/a_menu/koutou/it/h19/1321120.htm (japanese), 2012.

[7] Japan Intercultural consulting, available at http://www.japanintercultural.com/en/news/default.aspx?newsid=169

[8] IPA, http://www.ipa.go.jp/

[9] Steven Galbraith, available at http://www.isg.rhul.ac.uk/~sdg/ecc.html

[10] Intel, available at http://www.intel.com/content/www /us/en/processors/architectures-software-developer-manuals.html

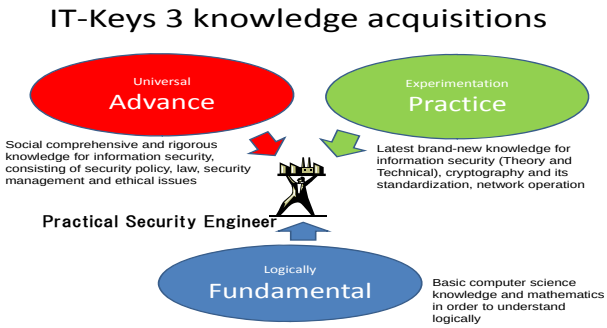


Figure 1. IT Keys' 3 knowledge acquisitions.

Figure 2. Exercise staff and learner responds to unexpected accidents.

Figure 3. Discussion in each group and presentation to CEO.

Figure 4. Exercise in dealing with security accidents using StarBED.

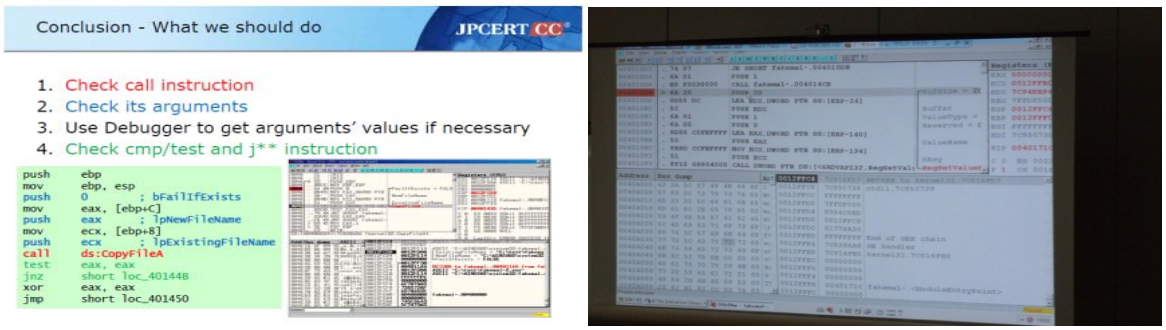


Fig.5 An assemble code for the malware static analysis.

 ISBN: 978-1-61208-231-8

Methodologies for detecting DoS/DDoS attacks against network servers

Mohammed Alenezi
School of Computer Science & Electronic Engineering
University of Essex name
Colchester, UK
mnmale@essex.ac.uk

Martin J Reed
School of Computer Science & Electronic Engineering
University of Essex name
Colchester, UK
mnmale@essex.ac.uk

***Abstract*—As denial of service (DoS) attacks are becoming more common in the Internet, there is greater need for solutions to overcome these attacks. Defending against DoS/ DDoS attacks can generally be divided into 3 phases: prevention, detection and response. Detection is one of the key steps in defending against DoS/ DDoS attacks. However, with the high variation in the DoS/DDoS attack types, the detection of such attacks becomes problematic. A good detection technique should have short detection time and low false positive rate. This paper presents an introduction to intrusion detection systems (IDS) and survey of different DoS/DDoS detection techniques. The key observation of this survey paper is that a CUSUM-based detection technique has many advantages over other statistical instruments in that it is non-parametric; consequently, it does not require training and is more robust to variations in the attack profile.**

Keywords-DoS; DDoS; detection; network security.

I. INTRODUCTION

As DoS attacks become one of the most threatening security issues, the need to detect this type of attack is increasing. DoS is not just a "game" played for fun by some attackers, it has become an effective weapon for cyber war or for so called "hacktivist" groups [1]. In general, detection is required before the spread of a DoS attack. DoS detection is often part of a wider intrusion detection system (IDS) [2, 3]. An IDS is best defined as software or hardware used to detect unauthorized traffic or activities that are against the allowed policy of a given network [4]. Intrusion detection is not a new research field, with one of the earliest published IDS papers in 1980 by Anderson [5]; in 1987, Denning [6] provided a structure for researchers working on IDS [2]. IDS can be classified based on the serving component (the audit source location) as either host-based, network-based or a combination of both. In a host-based IDS the audit information, such as application and operating system log files, are monitored while the network traffic is monitored in a network-based IDS. The host-based is usually located in a single host while the network-based system is usually located on machine separate from the hosts that it protects [7]. Hybrid intrusion detection systems combine both the network and host-based systems [8].

The rest of this paper is organized as follows. In section II, an overview of the IDS is presented, while in section III DoS detection is introduced. In section IV, general DoS classification is presented with different proposed techniques and discussion. The classification of DoS flooding-based attack is presented in section V. Our key observations about the detection techniques are presented in section VI.

II. IDS OVERVIEW

Network-based IDS (NIDS) usually detects attacks such as worms, scans, DoS attacks, botnets, and other types of attacks [9]. In the following, a general overview of the IDSs will be presented. Then, more precisely DoS detection techniques will be reviewed.

Network IDSs are generally categorized based on the detection method as one of two types: signature-based or anomaly-based detection. Signature-based, also known as rule- or misuse-based [10], detects an attack by comparing well-known attack signatures, or patterns, with the monitored traffic. A match generates an alarm for a potential attack. This type has fast detection time, detects most known attacks [11], and, generally has a low false positive rate, *i.e.*, it does not signal an alarm for legitimate traffic. On the other hand, an anomaly-based IDS, also known as behavior-based, operates by comparing the network traffic behavior against previous "normal" traffic behavior. Any deviation in the comparison is considered to be a sign of an attack. The system acquires a normal traffic profile, usually through training, and monitors the traffic for any differences with the normal profile [12]. The normal traffic behavior is classified into two types [11]: standard and trained. The standard is based on standard protocols and rules such as TCP handshaking connection [13] set up and how the attacker could perform a half connection attack. The trained traffic is used to determine a threshold value for future detection. There are many network anomaly-based systems and interested readers can refer to [11]. Anomaly detection can detect unknown attacks; however, it generally produces higher false positive rates than signature-based systems. Figure 1 summarizes the IDS classifications. In practice, systems may combine both signature and anomaly-based techniques.

In general, anomaly-based intrusion detection systems operate in three phases [14]: parameterization, training, and detection. In parameterization, the parameters of the system are defined. The model of the normal behavior of the traffic will be built in the training phase. In the detection phase, the traffic behavior is compared against that in the training phase. If the comparison exceeds a threshold value a detection alarm is triggered.

 ISBN: 978-1-61208-231-8

III. DoS Detection

A. Overview

DoS prevention using ingress filtering [15] can help in reducing some types of attacks such as spoofing IP addresses as used by attackers to hide their identity. However, reactive techniques are often required and here detection is needed to alert about the attack and perform some automatic action. A DoS/DDoS attack is considered to be just one type of attack that an IDS can react to and there are different types of network DoS including: overloading a service with seemingly legitimate requests and sending malformed packets, which aims to cause a failure of the service through some bug in the service. This paper considers the former rather than the latter type, as malformed packet-based DoS is relevant to general host-based security and can be filtered using a rule-based approach.

One of the key elements in DoS detection technique is the time of detection [16]. A good detection mechanism should detect the DoS attack before the service starts to be degraded. However, packets from an overloading type of DoS are often indistinguishable from those of legitimate users. This makes the detection difficult and increases the chance for a false positive, which is a critical problem in DoS detection. A good detection technique should react quickly and have a low false positive rate.

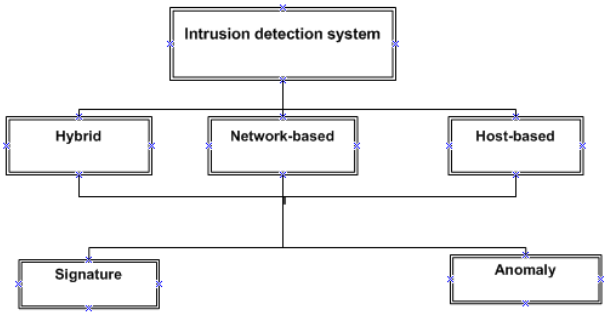


Figure 1. General classification of IDS

B. Classifications of DoS Detection

DoS detection techniques can be divided, as for general IDS, into signature and anomaly-based detection. Signature detection is based on well-known DoS attacks patterns [16], which are mostly malformed packets and protocol attacks. Anomaly detection is based on the traffic deviation from "normal" which is the form of most DoS attacks. The scope of this paper is anomaly-based DoS detection techniques for the overloading type of DoS [14]. However, even within this category, DoS detection techniques address different types of DoS attack such as a SYN flood attack[17] or a DNS attack [18, 19].

Different classifications have been proposed to provide a framework for the detection techniques. The differences are in the method used to detect the DoS attacks. Because of the paper length limitation, only three different proposed classifications were chosen. We have classified two works under general DoS detection classification and one under specific DoS flooding attack. A general description for each classification work will be presented, and some of the related techniques will be reviewed in the following sections.

IV. General DoS Classification

General DoS classification will cover two presented works. The first work was proposed by Peng [16]. The detection methods in this work were divided into: DoS attack specific detection and anomaly-based detection. DoS attack specific detection covers a general and wide range of different detection techniques types under one classification. In anomaly-based detection, the techniques are based on a comparison between the network traffic and a prepared normal traffic profile. The second work was proposed by Yonghua [17]. The detection techniques were divided into two types: IP attribute-based and traffic volume-based. The IP attribute-based technique monitors the behavior of selected IP attributes and considers the anomalies as deviations. The traffic volume-based studies the traffic of the network and applies statistical calculations on the packet rate of network flow.

A. Discussion

Peng [16] proposed two classifications for DoS detection techniques: DoS attack specific detection and anomaly-based detection. In DoS attack specific detection, the classification was made without regard to the methodologies in the detection; instead it was made to cover certain proposed techniques. For example, the authors have classified Multi Level Tree for Online Packet Statistics (MULTOPS) [20] and SYN detection techniques under the DoS specific detection. However, a closer inspection shows that it can be quite difficult to accurately classify such techniques. For example, the MULTOPS technique is quite different from the SYN detection technique, and it is not clear that the SYN is not, in fact anomaly-based detection.

Yonghua [17] proposed two classifications for DoS detection techniques: IP attribute-based and traffic volume-based. In IP attribute classification, certain parameters of the IP packets are monitored to detect the attack. For example, the source IP address, port number, or the time to live (TTL) value will be monitored as the values will show some change during an attack. In the IP attribute-based classification, the authors cover the techniques that deal with IP header parameters and emphasize the use of the TTL field. The traffic volume-based category covers any techniques that are not studying the IP header parameters. Many different methodologies placed in the traffic volume-based classification such MULTOPS, SYN detection, and other techniques that are based on statistical algorithms.

As mentioned earlier, signature-based detection is based on certain known characteristics in the traffic. Kompella [21] mentions that it is difficult to create a signature for a DoS attacks as the attackers could change the type and the content. Furthermore, Cheng [22] states that signature-based detection can be used to detect the communication between the attackers and their zombies. However, the communication could be encrypted making this detection

 ISBN: 978-1-61208-231-8

difficult. Consequently, Peng [16] states that signature-based detection is inefficient for DoS detection. However, we think signature-based should not be dismissed for the following reasons. First, although it is difficult to create signatures for all types of DoS, this fact applies to IDS more generally and not specifically DoS. There are certain types of DoS attacks that are straightforward to detect with a signature-based technique such as a TCP mixed flags attack. Second, Cheng [22] noted during the study one particular attack tool (Stacheldraht v1.666) that the communication between the attackers and the zombies can be detected using a signature-based approach. This is highly useful for the prevention stage. Consequently, while signature-based detection has limitation it can be highly effective in some cases.

The presented work by Peng [16] and Yonghua [17] provides a general classification for DoS detection techniques. Both of the works have different naming for the classifications and are overlapping in the mentioned techniques. In the following section, some of the proposed detection techniques will be reviewed.

B. Detection Techniques

A DDoS detection technique is proposed in [23], which is based on the source IP address. The system monitors the new source IP address of the packets instead of monitoring the traffic. The technique is based on the study by Jung [24], which indicates that during an attack, most of the source IP addresses are new. On the other hand, during flash crowds most of the IP addresses are not new. A flash crowd is a dramatic increase in the load on a web server by a, legitimate, large traffic surge causing an increase in congestion and packet loss [24]. The main drawback of this technique is that the attacker could launch a DoS attack by known (not new) IP addresses to the target to circumvent the detection system. The attacker can start normal communication with the target then perform the attack. Additionally, not all of the DoS attacks use spoofed IP addresses for example the attacker could use zombies with real IP addresses.

Talpade [25] proposes a detection technique based on the characterization of the dynamic statistical properties of the network traffic such as time to live (TTL) and other IP header information to detect the anomaly in the traffic. The characteristic of this idea is based on the change in the statistical distribution of the TTL values which indicates an anomalous change in the traffic. The main drawback is that the change in the TTL values does not always associate with anomalous traffic. Also, the model was not proposed for DDoS specifically.

Kim [26] proposes a detection technique based on creating a stable baseline profile to monitor the deviations in the traffic. An analysis was conducted to check the stability of the traffic with regards to different parameters. Significant differences in traffic patterns were found between different sites. Therefore, a baseline profile that is based on different attributes was proposed for detection. The choice of the attributes was based on the assumption that some of the attributes such packet size, TCP flag pattern, and protocol types can be anticipated by the attacker. On the other hand, based on the author's opinion, attributes such as TTL, source IP prefixes, and server port distribution are site dependent and difficult for the attacker to learn. Thus, the technique was proposed based on these attributes. The work presented in [26] has some drawbacks such as the chosen attributes are not directly related to DDoS attacks and there is added computational complexity with a high false positive rate [17].

Yonghua [17] proposed two DDoS detection techniques based on distance. Average distance estimation is the first one and the second is distance-based traffic separation. By analyzing the distance value and traffic rate, the attack can be detected. The TTL value is used to infer the distance value in the average distance estimation technique. The "normality" of the traffic is determined by the prediction of the mean value of the distance, where the prediction of the mean value was achieved by using the exponential smoothing estimation technique [27]. The second technique, distance-based traffic separation, uses the prediction of traffic arrival rates from different distances and thus the normality of the traffic is defined. The prediction of traffic arrival rates is achieved by using the minimum mean square error (MMSE) linear predictor technique. The normality and abnormality can be separated in the traffic for both techniques by using the mean absolute deviation (MAD).

Yonghua's techniques encountered the following drawbacks: first, the detection is based on the distance which is inferred from the TTL value. The distance will not reflect the real anomaly in the traffic. The attacker can know the distance to the victim and explicitly choose the path. Also, a sophisticated attacker can fix the TTL value to be within the predicted distance. Furthermore, the paths are subjected to change and different policies could be applied by different IPSs. Finally, for both of the techniques, the prediction of the normality of the traffic is achieved through the use of existing estimation techniques which are affected by the samples and can be anticipated by the attacker.

MULTOPS is proposed by Gil and Poletto [20]. It is a heuristic and data structure-based technique used by routers to detect a DDoS attack. The packet rate statistics for subnet prefixes are maintained by the nodes of the tree. The statistics are collected from different aggregate levels. The size of the tree is expandable with regards to the available memory. MULTOPS assumes the packet rate for the normal traffic in the communication between two machines is proportional. Therefore, any disproportional in the packet rate would trigger an alarm for the attack.

MULTOPS encounters some limitations mentioned by the authors. The location and set up of MULTOPS routers in the network would affect the ability of the technique to detect attacks with randomized IP source addresses packets. Legitimate packets for a certain IP destination address will be dropped as the MULTOPS would be confused by the spoofed IP address packets and identify the destination address to be under attacks. Furthermore, large number of attackers could connect to the victim in a normal way and the flows rate of the attackers' traffic is still proportional which means MULTOPS will not detect the attack. For example, large number of attackers could connect to the victim

 ISBN: 978-1-61208-231-8

through HTTP or FTP requesting a large file download. The victim will not be able to handle all of the requests consequently DoS and MULTOPS will not be able to detect the attack because the flow rate is proportional. Additionally, MULTOPS will suffer from a high false positive rate with streaming services as their flows are disproportional [16].

A detection technique for SYN flooding was proposed by Wang [28]. It is based on the normal behavior of TCP protocol (i.e. handshaking process and FIN or RST) and the sequential change point detection. The sequential change point detection is a statistical method to check for a change in a data [29]. To make the technique easy to use and more general, a non-parametric cumulative sum (CUSUM) method was used. The technique compares the ratio of SYN packets to the FIN or RST to find a change. One of the drawbacks of this technique that is the attacker could send the FIN or RST along with the SYN packet to avoid the detection [16].

A DoS detection technique was proposed by Blazek in [30]. The technique is based on statistical analysis on the data from different network layers to detect a change. The technique consists of two methods: adaptive sequential and batch sequential. The technique is based on the change point detection theory. To achieve a fixed rate of false alarms, statistical analysis of training data was utilized by both methods. The authors claim that their technique has three features: the methods are self-learning; the attacks can be detected with small delay; and computational complexity is manageable. The technique uses different traffic types such TCP and UDP in change detection modeling. The main drawback of the technique is the high computational complexity.

One of the key issues in DoS detection is how to discriminate between legitimate and attacker traffic to reduce the false positive rate. Cheng [31] proposes a technique, which is based on spectral analysis, to differentiate between normal traffic and attacker traffic. In order to use the spectral analysis in a packet-based network, a signal was defined as the number of arrival packets in a fixed length time interval. The power spectral density of the signal is estimated to discover the periodicity. Based on the fact that the periodicity around the round trip time of the normal TCP flows is strong in both directions while the attack flows are not, the attack is detected. The technique is not able to detect any attack other than TCP flows. Other protocols such UDP would pass undetected by the technique. A sophisticated attacker can send attack traffic at the same periodic interval to avoid detection such as low-DoS. The attack traffic does not have to be from a single source to form high volume. An attacker could use the zombies to send normal behavior traffic to the victim. However, the large number of zombies would be enough to overwhelm and deny the service from the victim [16]. Kulkarni [32] proposed a detection technique ,which is based on Kolmogorov complexity, to detect DDoS attacks. Kolmogorov complexity calculates the size of the smallest representation of the data and measures the degree of the randomness [33]. In general, it is based on the correlation between the traffic flows to distinguish between the attack traffic and high legitimate load traffic. It is been assumed that during the DDoS attack, the generated packets tend to have similar characteristics such as protocol type, destination address, type and execution pattern. All of the attack packets from different locations will have the same destination address which gives a similarity for the traffic pattern. This similarity can be detected by using the Kolmogorov complexity-based technique. On the other hand, the high load legitimate traffic tends to contain different types and characteristics which make the traffic flows to be randomly distributed and not greatly correlated. The technique is based on correlation and assumptions which are not always would be valid in case of the attack as the attackers can create a random flow to avoid the detection.

Cabrera [34] proposed a technique to proactively detect DDoS by using a time series analysis. The correlation between the traffic behavior at both of the victim and the attacker is the basis for this technique. A normal profile is built in order to compare any deviation in the traffic from the normal behavior to signal an attack alarm. In order to build the normal profile, key variables and correlation process need to be identified. Key variables are extracted at the victim side and then the variables, from the attackers, that are correlated to the extracted key variable are calculated by statistical tools such as Granger Causality Test (GCT) and Auto Regressive Model (AR Model) etc. For example, the key variable could be the ICMP echo packets at the victim and the variables correlation could be the ICMP replies [16]. To harden the detection process, different attack traffic could be combined in one type to make the correlation process is very complex as there will be many key variables to be correlated. It is been assumed that the same attack tool will be used from the sources of the attacks which is not always the case [16].

V. NETWORK BASED DOS FLOODING CLASSIFICATION

A survey for detecting DoS flooding-based attacks was presented by Carl [35]. The detection techniques are classified based on the algorithms used (not a certain parameter or behavior) into three groups: activity profiling, sequential change point detection, and wavelet analysis. Each group represents a general framework for the detection process.

A. Activity Profiling

Inside the header of the packet, certain information of the network traffic is monitored to generate an activity profile. The average packet rate for a network flow is defined as the activity profile. Consecutive packets with similar header fields such as protocol, port and addresses represent the network flow. The activity level or the average packet rate can be determined by the elapsed time between the consecutive matching packets. The average packet rates of all inbound and outbound flows are used to calculate the total network activity by dividing the sum over the average packet rates [35].

A high number of flows could be resulted by monitoring certain protocol services and this number will be increased for different services and protocols. Therefore, clustering concept was used to avoid the dimensional problems [35].

 ISBN: 978-1-61208-231-8

Individual flows with similar characteristics can be grouped in a cluster. The summation of constituent flows is used to determine the activity level of the cluster. The activity level of the clusters will be used to detect the attack based on an increase in the activity levels between the clusters which indicates an increase the attack rate. Distributed denial of service could cause an increase in the overall clusters.

The backscatter analysis project [36] is an example of the activity profiling. The authors were trying to estimate the worldwide DoS activity. During the attack, mostly the attacker uses packets with spoofed source IP addresses and when the victim replies to the spoofed source addresses, the packets will be backscattered. The backscattered packets are monitored and clustered based on the source address which is the victim's address. The normality of the distribution of the clustered backscattered packets, which is calculated by using Anderson-Darling test, is used to detect the attacks and define the threshold of the cluster's activity level.

Feintien [37] proposes an activity level DDoS detection technique. It is based on statistics and entropy of some of the IP header's attributes. For selected attributes such as IP source address, the entropy and Chi-square distribution are calculated for different cluster flows. Each cluster is categorized according to how frequent the source address of the packet has been seen. For example, the first cluster represents the most frequent source address seen in the traffic while the second holds the next 4 most seen source address. The third, fourth, and the fifth hold the next most 16, 256, and 4,096 source addresses respectively [35]. The last cluster will hold the rest of the traffic. Based on calculations, the DDoS can be detected by comparing the abnormal to normal traffic. The main drawback is the choice of the attribute that will be used for entropy calculation [17].

B. Sequential Change Point Detection

In sequential change point detection [35], the traffic is filtered at the victim, according to different criteria, such as address, port, and protocol. The filtered traffic is treated as a time series. For an attack starting at time $\mathcal{F}$, a change will be shown in the calculated statistics at time $\geq \mathcal{F}$. A Cumulative sum (CUSUM) [29] is one of the change point detection algorithms. It requires less computational and memory resources than other change point detection algorithms. CUSUM can be applied to DoS attacks by comparing the actual average for the traffic in the time series with the expected average. For a given time series sample, the difference between the actual and expected average is calculated. The CUSUM recursively will increase in case the difference exceeds an upper bound for attack traffic. On the other hand, the difference in the normal traffic will be under the bound and the CUSUM will be decreased. The DoS attack could be identified by defining a threshold that would specify the allowed increase in the time series within the upper bound. Based on the behavior of the network such as the expected volume of traffic or the range of delay that can be tolerated or the sensitivity of the running applications, CUSUM algorithms can trade-off between the detection delay and false positives rates during the setting of the threshold and the upper bound [35].

C. Wavelet Analysis

The input signal, in wavelet analysis, is described as spectral components in wavelets. With wavelets, the time for a given frequency can be determined as the wavelets provide a description for concurrent time and frequency. On the other hand, the Fourier analysis provides only a frequency description [35]. The time-localized anomalous signals can be separated from the noise signals by wavelets. By analyzing each spectral window's energy, the anomalies can be determined.

Paul *et al.* [38] proposed a detection technique based on wavelet analysis. The analysis was applied to four anomaly types: measurement failure, attacks, flash crowds, and outages such as network failures. The data used for the analysis was collected on a border router of a large university over six months. The data consists of IP flow and SNMP [39] measurements, which are decomposed into different time series. High and mid- band spectral energies are presented by applying wavelets on each time series.

VI. KEY OBSERVATIONS

As a result from reviewing the presented work on IDS and DDoS detection, key issues were observed which could help in studying DoS/DDoS detection. We believe that there are many aspects that should be considered towards getting a reliable detection system. It is not only depending on the technical details of the detection technique, other issues should be considered such as the following. First, the location of the machine that will carry on the detection process is vital and related to the design of the system. It could be a host-based where the traffic received and analyzed by the host or a network-based where the network traffic is monitored by a separate dedicated machine. Another choice is a hybrid system which combines both host and network types. Based on the protected system (protected system points to the system that installed the IDS), the location should be considered. For example, protecting a single server is different from protecting an ISP network that includes many hosts, servers and network resources. Second, considering the nature of the service provided by the protected system is part of the good design. Protecting a web server is different from protecting database server in terms of the information sensitivity, response time and the availability of server. Third, the choice for the used methodology such as anomaly-based or signature-based would make a difference. The choice should be based on the nature of the expected traffic and type of service provided by the protected system. For example, if the system is connected to the Internet or locally to private networks. There is a trade-off between anomaly-based and signature-based detection methodologies. Table I shows a comparison between the two methodologies. The same can be applied to DoS/DDoS detection. In DoS/DDoS, the detection is divided into two phases: the selected attributes to be monitored and the statistic methods. The selected attributes should show different behavior during the attack. The statistic methods would discover the abnormality in the selected attribute. Choosing adequate attributes would make significant difference in detection

 ISBN: 978-1-61208-231-8

time. Additionally, choosing the right statistic method among the wide available range would help in discovering the abnormality in the attribute very fast.

In the experience of the authors, the CUSUM statistical techniques perform better than other statistical techniques due to many reasons. First, CUSUM is a non-parametric technique which means training traffic is not required to detect the change in the traffic such as Kolmogorov complexity [33], Granger Causality Test (GCT) and Auto Regressive Model (AR Model) [34]. Second, CUSUM requires less computational and storage resources comparing to other statistical techniques. It only requires defining bounds and threshold value to detect the change in the traffic behavior. Defining the bounds and threshold depends on type of running service and traffic.

TABLE I. SIGNATURE AND ANOMALY BASED COMPARISON

Method	Detection time	Reliability	Detect new attacks	False Positive	Requirements
Signature	Fast	Yes	No	Very low	Well-known signature
Anomaly	vary	Yes	Yes	High	Trained data

VII. CONCLUSION

DoS/DDoS is one of the main security threats in the Internet. Defending against DoS/DDoS becomes a necessary step that must be considered by the companies and ISPs. DoS/DDoS detection is regarded to be one of the main phases in overcoming the DoS/DDoS problem. IDS is used to detect different types of intruders including DoS/DDoS attacks. An overview and broad classification IDS are presented. The difficulties and characteristics of DoS/DDoS attacks are discussed in the DoS detection section. Furthermore, a classification of DoS attacks is explained. Three different classifications have been chosen and divided in two groups: general DoS classification and network flooding DoS-based. In each classification, many different proposed techniques are introduced and reviewed to point out the limitations. A key observation of the authors is that while signature-based detection has limitations it should not be ignored as it is relatively efficient. In terms of the statistical techniques for anomaly-based detection, the CUSUM approach has many advantages over more sophisticated statistical instruments in that it is non-parametric and thus training is more straightforward.

REFERENCES

[1] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Computer Communication Review, vol. 34, pp. 39-53, 2004.

[2] J. McHugh, A. Christie, and J. Allen, "Defending yourself: The role of intrusion detection systems," Software, IEEE, vol. 17, pp. 42-51, 2000.

[3] D. Wagner and P. Soto, "Mimicry attacks on host-based intrusion detection systems," 2002, pp. 255-264.

[4] T. M. Wu, "Intrusion Detection Systems " Information Assurance Technology Analysis Center (IATAC), Septemper 2009.

[5] J. P. Anderson, "Computer security threat monitoring and surveillance," 1980.

[6] D. E. Denning, "An intrusion-detection model," Software Engineering, IEEE Transactions on, pp. 222-232, 1987.

[7] M. V. Mahoney and P. K. Chan, "Learning nonstationary models of normal network traffic for detecting novel attacks," 2002, pp. 376-385.

[8] H. Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of intrusion-detection systems," Computer Networks, vol. 31, pp. 805-822, 1999.

[9] A. Sperotto, et al., "An overview of IP flow-based intrusion detection," Communications Surveys & Tutorials, IEEE, vol. 12, pp. 343-356, 2010.

[10] F. Dressler, G. Munz, and G. Carle, "Attack detection using cooperating autonomous detection systems (CATS)," Wilhelm-Schickard Institute of Computer Science, Computer Networks and Internet, 2004.

[11] S. A. Khayam, et al., "A survey of anomaley-based intrusion detection systems," School of Electrical Engineering and Computer Science (SEECS), National University of Sciences & Technology (NUST)2009.

[12] N. Ye, Secure computer and network systems: modeling, analysis and design: Wiley, 2008.

[13] R. W. Stevens, TCP/IP illustrated, Volume 1: The protocols: Addison-Wesley Professional, 1994.

[14] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez, and E. Vazquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," computers & security, vol. 28, pp. 18-28, 2009.

[15] ArborNetworks, "Worldwide Infrastructure Security Report," Feb 2012.

[16] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," ACM Computing Surveys (CSUR), vol. 39, p. 42 pages, April 2007.

[17] Y. You, M. Zulkernine, and A. Haque, "Detecting flooding-based DDoS attacks," 2007, pp. 1229-1234.

[18] R. Naraine. Massive DDoS attack hit DNS root servers [Online]. Available:http://www.esecurityplanet.com/trends/article/0,10751,1486981,00.html.

[19] M. Prince. Deep Inside a DNS Amplification DDoS Attack [Online]. Available:http://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack

[20] T. M. Gil and M. Poletto, "MULTOPS: a data-structure for bandwidth attack detection," in Proceedings of 10th Usenix Security Symposium, 2001, pp. 23-38.

[21] R. R. Kompella, S. Singh, and G. Varghese, "On scalable attack detection in the network," in Proceedings of the 4th ACM SIGCOMM Conference on Internet Measurement. ACM Press, , New York, 2004, pp. 187-200.

[22] G. Cheng, "Malware FAQ: Analysis on DDOS tool Stacheldraht v1. 666,"[Online].Available:http://www.sans.org/resources/malwarefaq/stacheldraht. php, 2006.

[23] T. Peng, C. Leckie, and K. Ramamohanarao, "Proactively detecting distributed denial of service attacks using source IP address monitoring," NETWORKING 2004. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications, pp. 771-782, 2004.

[24] J. Jung, B. Krishnamurthy, and M. Rabinovich, "Flash crowds and denial of service attacks: Characterization and implications for CDNs and web sites," 2002, pp. 293-304.

[25] R. Talpade, G. Kim, and S. Khurana, "NOMAD: Traffic-based network monitoring framework for anomaly detection," in Fourth IEEE Symposium on Computers and Communications, 1999, pp. 442-451.

 ISBN: 978-1-61208-231-8

[26] Y. Kim, J. Y. Jo, and K. K. Suh, "Baseline profile stability for network anomaly detection," International Journal of Network Security, vol. 6, No.1, pp. 60–66, Jan 2008.

[27] V. Jacobson, "Congestion avoidance and control," in Proceedings of SIGCOMM'88, ACM, 1988, pp. 314-329.

[28] H. Wang, D. Zhang, and K. G. Shin, "Detecting SYN flooding attacks," in In Proceedings of IEEE INFOCOM, 2002, pp. 1530–1539.

[29] M. Basseville and I. V. Nikiforov, Detection of abrupt changes: theory and application vol. 15: Prentice Hall Englewood Cliffs, 1993.

[30] R. B. Blazek, H. Kim, B. Rozovskii, and A. Tartakovsky, "A novel approach to detection of denial-of-service attacks via adaptive sequential and batch-sequential change-point detection methods," 2001, pp. 220-226.

[31] C. M. Cheng, H. Kung, and K. S. Tan, "Use of spectral analysis in defense against DoS attacks," 2002, pp. 2143-2148 vol. 3.

[32] A. B. Kulkarni, S. F. Bush, and S. C. Evans, "Detecting distributed denial-of-service attacks using Kolmogorov complexity metrics," TR176, GE Research Center, 2001.

[33] M. Li and P. M. B. Vitányi, An introduction to Kolmogorov complexity and its applications: Springer-Verlag New York Inc, 2008.

[34] J. B. D. Cabrera, et al., "Proactive detection of distributed denial of service attacks using mib traffic variables-a feasibility study," 2001, pp. 609-622.

[35] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," Internet Computing, IEEE, vol. 10, pp. 82-89, 2006.

[36] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," ACM Transactions on Computer Systems (TOCS), vol. 24, pp. 115-139, 2006.

[37] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical approaches to DDoS attack detection and response," in Proceedings of DARPA Information Survivability Conference and Exposition, 2003, pp. 303-314 vol. 1.

[38] P. Barford, J. Kline, D. Plonka, and A. Ron, "A signal analysis of network traffic anomalies," in Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment, New York, NY, USA, 2002, pp. 71-82.

[39] W. Stallings, SNMP, SNMPv2, SNMPv3, and RMON 1 and 2: Addison-Wesley Longman Publishing Co., Inc., 1998.

 ISBN: 978-1-61208-231-8

An In-Depth Analysis of the Security of the Connected Repair Shop

Pierre Kleberger, Tomas Olovsson, and Erland Jonsson
Department of Computer Science and Engineering
Chalmers University of Technology
SE–412 96 Gothenburg, Sweden
Email: {pierre.kleberger,tomas.olovsson,erland.jonsson}@chalmers.se

***Abstract*— In this paper, we present a security analysis of delivering diagnostics services to the connected car in future connected repair shops. The repair shop will mainly provide two services; vehicle diagnostics and software download. We analyse the security within the repair shop by applying a reduced version of the threat, vulnerability, and risk analysis (TVRA) method defined by ETSI. First, a system description of the repair shop is given. Security objectives and assets are then identified, followed by the threat and vulnerability analysis. Possible countermeasures are derived and we outline and discuss one possible approach for addressing the security in the repair shop. We find that many of the identified vulnerabilities can directly be mitigated by countermeasures and, to our surprise, we find that the handling of authentication keys is critical and may affect vehicles outside the repair shop as well. Furthermore, we conclude that the TVRA method was not easy to follow, but still useful in this analysis. Finally, we suggest that repair shop security should mainly be addressed at the link layer. Such an approach may integrate network authentication mechanisms during address allocation and also support encryption of data for all upper layer protocols with minimal modifications.**

Keywords-security analysis; vehicle diagnostics; connected car.

I. INTRODUCTION

The ongoing trend with equipping vehicles with wireless access will bring many new services into the vehicle. Mainly, these services are used when the vehicle is on the road, but there are also other cases when a wireless connection to the vehicle is useful. One is the usage of WiFi-technology to connect the vehicle to a repair shop. A wireless connection between the vehicle and the repair shop has many benefits [1]; no cables are needed, which shorten the time for connecting the vehicle to the repair shop, and also makes it possible to connect more vehicles at the same time, e.g., to update the firmware in several vehicles at the same time. However, using WiFi-technology, where many vehicles can connect to the same wireless Access Point (AP), also raises security related questions; how does the mechanic know that she is working with the right vehicle, and what support is implemented in the network to protect the vehicle against malicious network behaviour? For example, Checkoway et al. [2] have already demonstrated some security issues with the PassThru-device used for connecting the in-vehicle network to the WiFi-network. When the PassThru-device was compromised, malicious software was installed in the device, which attacked the connected vehicle. As the vehicle is safety critical, it is crucial that such attacks are prevented in the repair shop.

Two services are mainly requested in the repair shop, vehicle diagnostics and software download. In this paper, we assess the security within the repair shop when vehicles are connected to the repair shop using wireless connections. The analysis is performed by applying a reduced version of the Threat, Vulnerability, and Risk Analysis (TVRA) method proposed by ETSI [3] as it has been used for evaluating the emerging Intelligent Transportation Systems (ITS) architecture [4]. Originally, ETSI defined this method for use by their standards developers to analyse telecommunication systems [3]. Even though this is a rather limited setting, we believe that results from such an analysis, not only will derive security mechanisms for this environment, but also can be used for secure vehicle diagnostics, software download, and possibly other services in a larger more generalised environment.

The rest of this paper is outlined as follows. Section II presents the related research within the area. The analysis method, together with an overview of the repair shop and its services, are given in Section III. In Section IV, the model of the repair shop network is described followed by the security objectives in Section V. An inventory of assets is established in Section VI. Threats and vulnerabilities are then identified and the countermeasures are derived in Section VII and VIII, respectively. These countermeasures are then used in Section IX for discussing one possible approach for addressing the security. The paper closes with a discussion and proposal for future work in Section X and our conclusion in Section XI.

II. RELATED WORK

Even though much effort has been spent on research in the vehicular communication (VC) domain [5], most of the work during the last decade has been directed towards systems for ensuring the safety of the vehicle and less towards security. However, the effort in addressing security of VC systems seems to have increased during the last few years. Both the SeVeCOM project [6] and the EVITA project [7] have been addressing security with focus on communication between vehicles and within the vehicle, respectively. In the SeVeCOM project, a security architecture for VC systems was developed, and one of the outcomes was the three security services of secure beaconing, secure neighbour discovery, and secure

 ISBN: 978-1-61208-231-8

geocasting [8]. Methods for handling identification and privacy (by help of pseudonyms) using certificates and how to revoke these were also proposed.

Efforts in defining a standardized platform for ITS applications have also been spent [9, 10] and the security for such an ITS architecture has also been evaluated [4, 11]. Both software download and remote diagnostics are included as applications of this ITS platform [12]. However, in this paper, we look at the vehicle diagnostics as a stand alone service within the repair shop, outside the scope of the ITS platform. We extend the Local Area Network (LAN) in the repair shop with a wireless connection to the vehicles. Hence, we assess security within a local network without Vehicle-to-Vehicle (V2V) communication. Vehicles connect to and disconnect from the local network and local network devices are included in the assessment.

Specialised approaches for providing secure software download and firmware updates to vehicles have been proposed [13–15]. In these approaches, protocols for secure software download have been described, protocols that can cope with arbitrary distance between the vehicle and the software supplier. Furthermore, methods for ensuring that the firmware is flashed correctly have also been proposed [16, 17]. These approaches are specific to the delivery of ECU firmware and do not include remote diagnostics. In this paper, the delivery of ECU firmware is an integrated part of the vehicle diagnostics protocol.

Idrees et al. [18] give a detailed presentation of a remote software download procedure including some remote diagnostics, which utilises the hardware security module (HSM) designed within the EVITA project. Mechanisms for exchanging necessary keys between EVITA-enabled devices and for protection of transmitted data are described. However, we take a broader perspective by assessing the security of the whole repair shop network.

A risk assessment of the wireless communication infrastructure between the backend system, used for providing diagnostics service and firmware, and the vehicle was performed by Nilsson et al. [19]. In their analysis, they target end-to-end communication between the backend system and the vehicle, while we consider the whole repair shop network and the included devices.

Efforts are also made by ISO to create a standardized diagnostics protocol, Diagnostics over IP (DoIP) [20], and some initial tests have been performed by Johanson et al. [21]. However, appropriate security mechanisms are still missing in the DoIP-protocol.

III. Background

A. The Repair Shop

In our previous work [22], we proposed a model of the connected car infrastructure to clarify the possible communication paths with future connected vehicles. To derive a model of the repair shop for our analysis in this paper, this previously proposed model was used. An overview of the repair shop is shown in Figure 1.

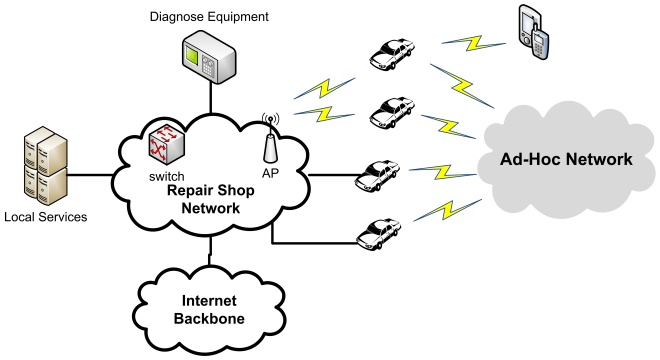
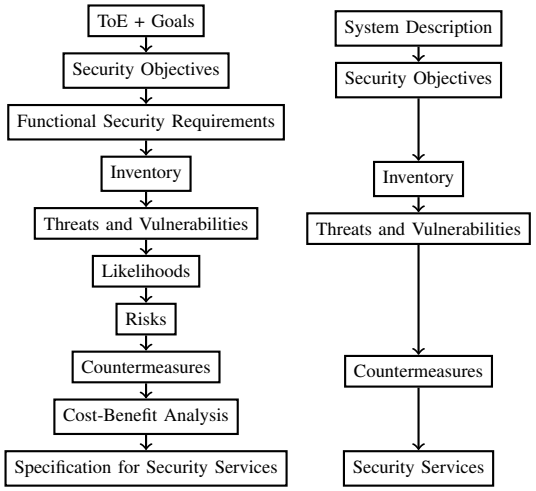


Figure 1. Overview of the repair shop



(a) TVRA method (b) Analysis method used

Figure 2. Overview of analysis methods

We consider the repair shop network to be trusted. Multiple vehicles are connected to this network, both with wired and wireless connections, as well as the diagnostics equipment and local servers providing necessary services to the LAN (e.g., DHCP [23]). The internal network at the repair shop contains wireless APs, Ethernet switches, and a connection to the Internet. Furthermore, the vehicles in the repair shop can communicate directly with other vehicles or devices through an ad-hoc network.

B. Analysis Method

For our analysis, we apply a subset of the TVRA method proposed by ETSI [3]. An overview of the method and our subset is shown in Figure 2. We will first summarise the complete method and then discuss the parts left out.

The TVRA method [3] can briefly be summarised as follows; The *target of evaluation (ToE)* is identified and the assets within are described together with the goals of the evaluation. *Security objectives* are then identified and classified based on the five security attributes: confidentiality, integrity, availability, authenticity, and accountability (CIAAA). These security objectives are then used to derive the *functional*

 ISBN: 978-1-61208-231-8

security requirements. Then, an *inventory of assets* is done. Possible *vulnerabilities* are then identified and classified together with their *corresponding threats* and their unwanted outcome. These threats are classified based on the following four categories: interception, manipulation, denial of service, and repudiation. *Risks* are then calculated depending on the *likelihood* of these threats and their unwanted outcome. Finally, a set of *countermeasures* are derived and a *cost-benefit analysis* is performed to select the most suitable ones to *reduce the risks* of the identified threats. These results are then used to design the *security services*.

Four steps in the TVRA method are omitted in our analysis: deriving the *functional security requirements* and calculations related to *likelihoods*, *risks*, and *cost-benefit analysis*. The functional security requirements are a more detailed specification of the security objectives and include descriptions of how a certain security objective should be addressed in the implementation, e.g., that access control should be implemented by means of a username and password. Since we want to find general security mechanisms and not limit the analysis to a single security implementation, we leave this step out. Furthermore, we do not want to calculate any likelihoods, nor risks for the different threats and vulnerabilities and it will therefore be up to an implementor to make a trade-off and choose the best countermeasures and security services for their settings.

IV. System Description

A. Network Model and Assumptions

A more detailed model of the repair shop network is shown in Figure 3. We assume that a set of diagnostics equipment, $\{D_1, D_2, ...\}$, and vehicles, $\{V_1, V_2, ...\}$, are connected to the repair shop network, using wireless and/or wired connections. The diagnostics equipment can be either dedicated hardware or a general computer used to perform vehicle diagnostics. A local server, LS, is also available to provide necessary services and to maintain the LAN, e.g., DHCP for dynamic IP address allocation. Furthermore, we assume that other devices, which are needed to run the business and not to maintain cars, are connected to the network using wired connections. These devices, denoted office hosts, cannot be excluded from the model, since they need network connectivity in order for employees to, e.g., read emails and write documents. However, these computers may be potentially threatening to the communication with the vehicles if misused or being compromised. These office hosts are marked with the grey box in Figure 3.

B. Vehicle Diagnostics Scenario

The scenario of performing vehicle diagnostics can be divided into the following three steps. First, the vehicle arrives to the repair shop and *connects to the wireless AP*. If the vehicle lacks wireless access, the vehicle is connected to the wired network by a mechanic in the repair shop. Then, when the link is established, the vehicle needs to *announce its presence* in the network, so that the diagnostics equipment can find it [24]. Finally, the diagnostics equipment can initiate a *diagnostics session* with the vehicle and perform its tasks, e.g., diagnose an Electronic Control Unit (ECU) or update the firmware of an ECU.

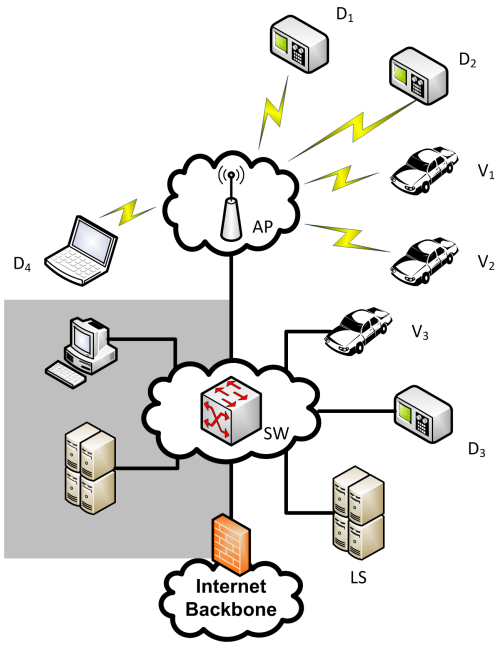


Figure 3. Model of the repair shop network

C. Definitions

The following definitions are used in this paper:

Diagnostics session. An established connection between diagnostics equipment and a vehicle.

Diagnostics data. Data, transmitted or stored, associated with a diagnostics session. Diagnostics data is classified as confidential or non-confidential, where *non-confidential is assumed* unless otherwise stated.

ECU firmware. Program code installed in non-volatile memory of ECUs.

Confidential data. Diagnostics data classified as confidential and ECU firmware.

Core network traffic. Network communication necessary to maintain the network infrastructure, i.e., ARP, DHCP, DNS, and ICMP.

Authorised device. A device is an authorised device if it fulfils one of the following requirements:

(1) a vehicle, which has been connected to the network by a mechanic, who thereby authorises the vehicle, using a cable or wireless connection, or
(2) a vehicle, which has been authorised by a trusted party to connect to the repair shop network, e.g., a service booking system giving the vehicle authorisation to connect to the network at a reserved service time, or
(3) diagnostics equipment, or
(4) any other device needed to diagnose a vehicle.

 ISBN: 978-1-61208-231-8

Note that office hosts are not included in the definition of an authorised device. A clear distinction between the devices in the repair shop is made, where authorised devices are those that take part in vehicle diagnostics.

D. Limitations

The following limitations are assumed in this paper:

1) Even though the in-vehicle network is not secure, we assume that the communication within the vehicle is correctly transmitted.
2) Denial of service (DoS) attacks against the network are not addressed. Other security systems, e.g., Intrusion Detection Systems (IDSs), are needed to identify such activities, which we believe would be too costly and too complicated to manage for a repair shop.
3) Theft of physical assets. The physical assets are not considered to be of great value, but logical assets are (see Table I).

V. Security Objectives

The following security objectives are identified:

O1: To ensure the availability of the repair shop network, only office hosts and authorised devices should be given access to the repair shop network.

O2: Authorised devices must properly verify and validate the source of diagnostics data.

O3: Logical assets and diagnostics data must be protected against unauthorised modification.

O4: Logical assets must not be revealed to unauthorised parties.

O5: Only the following communication scenarios should be allowed in the repair shop network:

(1) devices may process core network traffic in the repair shop;
(2) diagnostics sessions may only be established between vehicles and diagnostics equipment;
(3) diagnostics equipment may connect to any device in the repair shop and to backend servers at the automotive company via the Internet connection;
(4) office hosts may establish connections with office hosts and the Internet, and process traffic from diagnostics equipment.

These security objectives include some important scenarios. For example, it is important that only authorised vehicles are allowed to connect to the network (O1), so that vehicles, when they are passing the repair shop, cannot connect to the wireless AP. Another example is, that certain types of communication should be prevented (O5), such as car-to-car communication inside the repair shop network; if vehicles are allowed to communicate with each other, an attacker may utilise this possibility to try to infect other vehicles with malicious software. However, since we are only concerned with protecting authorised devices, office hosts may communicate with other office hosts and the Internet, and process traffic from diagnostics equipment, so that a mechanic can retrieve necessary data to the diagnostics equipment.

Table I
Assets to protect

(a) Physical assets

ID	Model Reference	Asset
A_{P1}	V_x	vehicle
A_{P2}	D_x	diagnostics equipment
A_{P3}	AP	wireless access point
A_{P4}	SW	Ethernet switch
A_{P5}	LS	local server

(b) Logical assets

ID	Asset	Physical Assets
A_{L1}	authentication data and cryptographic keys stored in physical assets	A_{P1}, A_{P2}, (A_{P3}), (A_{P4}), A_{P5}
A_{L2}	diagnostics data that is considered confidential	A_{P1}, A_{P2}, A_{P5}
A_{L3}	ECU firmware	A_{P1}, A_{P2}, A_{P5}

It is also important to note that O1 only states that the repair shop should identify and authorise devices to connect to the repair shop network, but says nothing about how and whether the connecting device will verify the network. Hence, from the perspective of the network, it is important to make sure that availability is ensured by not giving access to unauthorised devices. However, from the perspective of the device, it is not important if it connects to a repair shop network or not, as long as O2 is ensured. The device will still only accept communication from sources it can validate.

VI. Inventory of Assets

The assets to protect are divided into two categories, physical assets and logical assets. The identified physical assets are listed in Table Ia and the logical assets, together with the associated physical asset, are listed in Table Ib. As already mentioned, in this paper we only deal with threats against the logical assets.

VII. Threat and Vulnerability Analysis

An analysis of possible vulnerabilities in the repair shop has been conducted. We will summarise the vulnerabilities here and highlight some important issues. For details, we refer to Appendix A.

A. Identified Vulnerabilities

Fourteen (14) vulnerabilities were identified. These were classified based on the five threat categories defined by the TVRA method [3]: eavesdropping, unauthorised access, masquerading, forgery, and information corruption.

- *eavesdropping (1).* Since malicious devices may eavesdrop on network traffic, weak protection of confidential data may lead to data disclosure.
- *unauthorised access (6).* Among the six vulnerabilities identified, three were the results of weaknesses in authentication and two due to software bugs. The last vulnerability was the result of issues regarding traffic separation. Due to weak authentication mechanisms and

Table II
POSSIBLE COUNTERMEASURES

	Countermeasure	Threat Category	Weakness
1	encryption	interception	weak protection of confidential diagnostics data and ECU firmware
2	(1) PKI + certificates (2) Kerberos	unauthorised access	(a) weak authentication (b) lack of proper authentication for wireless connections
		masquerade	lack of proper device identification
3	(1) logical traffic separation (2) cryptographic traffic separation (3) firewalls	unauthorised access	(a) lack of traffic separation (b) software bugs
4	(1) digital signatures (2) message authentication codes	forgery	(a) lack of data authentication (b) weak integrity check of diagnostics data (c) weak integrity check in vehicle ID broadcast
		information corruption	weak integrity check of diagnostics data
5	timestamps	forgery	lack of freshness in diagnostics session

software bugs, an attacker may circumvent authentication mechanisms or install malware, leading to disclosure of confidential data and modification of stored data. Furthermore, by circumventing the protection mechanisms to establish a wireless connection, an attacker may also get unauthorised access to the repair shop network.

- *masquerading (2).* Due to lack of proper device identification, an attacker may impersonate as another device and manipulate data or acquire confidential data. Even worse, if an attacker is in possession of proper authentication keys, for example, by a previous theft, the attacker can act as an authorised device.
- *forgery (4).* Due to the lack of data authentication and integrity checks, an attacker may fabricate and inject malicious data into diagnostics sessions. This may lead to problems such as wrong vehicle IDs being presented to the diagnostics equipment. Furthermore, replay of earlier diagnostics sessions may be possible, which may lead to dangerous situations, e.g., an attacker replays commands of her choice from a recorded diagnostics session.
- *information corruption (1).* Malicious devices may modify the data that pass through them. Therefore, weak integrity checks of diagnostics data can lead to malicious data being processed or stored in the vehicle. To ensure the safety of the vehicle, it is of outmost importance that such modifications are prevented.

We find that the exploitation of some of the vulnerabilities results in that logical assets can be acquired or that data can be illicitly modified.

B. Consequences of Lost and Modified Logical Assets

The loss of logical assets can have a major security impact. For confidential diagnostics data and ECU firmware, these might get copied, and for authentication keys, the loss of these can cause great damage. For example, if authentication keys to the diagnostics equipment are copied, an attacker may be able to impersonate as diagnostics equipment and connect to vehicles anywhere outside the repair shop. If there are no other authorisation mechanisms which protect the vehicle from accepting seemingly valid diagnostics sessions, the attacker can initiate new diagnostics sessions to vehicles until these authentication keys expire or are invalidated. Considering the number of vehicles these keys may give access to, the possibility of large scale attacks should not be neglected.

Modification of data can be critical. For example, if the ECU firmware can be modified, an attacker may change the behaviour of the vehicle in any way she desires.

VIII. COUNTERMEASURES

From the vulnerabilities found and discussed in the previous section, possible countermeasures against these were identified and grouped together based on the threats and weaknesses they address. These are presented in Table II. The following countermeasures were identified:

1) Encryption can be used to protect confidential data against eavesdropping. Furthermore, to prevent access to this data in intermediate storage, it can also be stored encrypted.
2) Strong authentication is needed. Private/public keys, with or without certificates, and Kerberos-like authentication mechanisms [4] can be used. However, precaution needs to be taken in case of lost keys. Either the keys should have a short lifetime and procedures for updating these are needed, or the keys have a longer lifetime and procedures for revoking them are needed.
3) Several possible countermeasures can be used to handle the lack of traffic separation within the repair shop network and to deal with misbehaving software. Traffic separation can be achieved either by logical separation or cryptographic separation. Logical separation can be implemented using virtual LAN (VLAN)-technology together with network mechanisms that only allow communication between connected hosts and the uplink [25]. For cryptographic separation, communication can be split into groups of allowed devices, where each group shares a session key. Furthermore, network filters, i.e., firewalls, can be used to limit network access so that software only is accessible to those devices that need it. Thereby, the exposure of software bugs is also limited.

 ISBN: 978-1-61208-231-8

4) Digital signatures and message authentication codes (MACs) can be used to verify the source of and the integrity in the communication, so that forgery and corruption of data can be detected. Furthermore, the digital signature or MAC should be created by the ultimate source of the communication and verified at the final destination so that possible modification in intermediate storage can be detected, e.g., ECU firmware should be signed by the software supplier and verified in the target ECU.
5) Timestamps in transmitted data can be used to prevent the possibility of replay attacks.

IX. Security Services

Based on the identified countermeasures, different approaches in securing the repair shop network are possible. In this section, we will outline one approach and discuss how this approach fulfils the security objectives, as well as how all identified threats and vulnerabilities are addressed.

We note that security objective O5 limits the possible communication scenarios in the repair shop network and that there are different approaches to address this. Depending on which approach is chosen, it will affect the architecture and thereby the implementation of the security mechanisms. Traffic separation is therefore discussed first, so that the architecture for other security mechanisms is defined.

A. Traffic Separation

To address security objective O5, the use of logical traffic separation or cryptographic traffic separation are possible. Since logical traffic separation, using for example VLAN-technology, depends on the equipment and communication technology used, we believe that such an approach is limited; it may not work in all environments, it needs to be maintained by someone with knowledge about the technology, and it is easy to make mistakes. The use of cryptographic separation, on the other hand, can be independent of the underlying communication technology and limited knowledge of the underlying protocols is needed. We therefore suggest that the security mechanisms addressing O5 should be implemented using cryptographic traffic separation.

Cryptographic traffic separation can be implemented at different communication layers, e.g., the network layer or the link layer. We suggest that it should be deployed at the lowest common communication layer, which is the link layer. With this approach, malicious traffic will progress through as few communication layers as possible, limiting the possibility of utilising software bugs in the network stack. Furthermore, encryption at link layer also addresses security objective O4, protection of logical assets, and vulnerabilities VU1 and VU5, and to some extent VU2, VU3, VU6–VU12, and VU14.

The details of how such a link layer encryption protocol should be implemented, needs to be investigated further. However, one interesting approach of applying link layer encryption in LANs has been implemented and demonstrated in the Linux operating system [26].

B. Authentication

Both public key infrastructure (PKI) with certificates and centralised authentication schemes are possible authentication mechanisms to address security objective O1 and vulnerabilities VU2–VU4, VU8, and VU9. However, we note that PKI together with certificates have already been discussed for usage in Inter-Vehicle Communication (IVC) [27]. Although we leave the choice of authentication protocol open to the implementor, special attention is needed regarding loss of authentication keys, as discussed in Section VII-B.

Since loss of the authentication keys used by the diagnostics equipment may give an adversary full access to vehicles, additional security mechanisms are needed. Thus, the vehicle should only accept diagnostics sessions when such a session is expected. A possible approach could be to use an authorisation mechanism where the authorisation is initiated by the vehicle's owner and not by the network. Another approach would be to use temporary authentication keys for diagnostics equipment, which are issued for a certain diagnostics session by some trusted third party.

An interesting outcome of using cryptographic traffic separation at the link layer, is the possibility not to use authentication mechanisms in wireless APs. Instead, authentication is performed at the link layer, between the connecting device and the DHCP service at the local server, during the process of IP-address assignment. Approaches for DHCP authentication have been proposed as part of link layer security protocols [26, 28], but need to be adapted to our context. For example, key management needs to adapted with respect to the amount of vehicles that may connect to the repair shop and that these vehicles may use different repair shops over time. Also, the authorisation process to the repair shop network needs to be adapted. This approach would remove vulnerability VU4, since encryption keys in the wireless AP will not be needed any more.

C. Data Integrity

Both digital signatures and MACs are possible to use. However, we leave the choice to the implementor. What is important regarding the chosen algorithm and its implementation, is that it ensures end-to-end integrity protection, so that data cannot be modified in any intermediate storage. Security objectives O2 and O3 and vulnerabilities VU10–VU14 are addressed here.

D. Firewalls

Firewalls should be used in the Internet gateway, in front of office hosts or in each of them, and in authorised devices in order to further restrict access to and between devices in the repair shop network. This would partly addresses vulnerability VU5–VU7.

X. Discussion and Future Work

In our work, we have chosen to follow a reduced version of the TVRA method to analyse the security of the repair shop network. The main reason for this choice was that the

 ISBN: 978-1-61208-231-8

TVRA method is used by ETSI in their ITS architecture standardisation process. Even though the repair shop network can be considered to be a rather limited system, the TVRA method has not been easy to follow and apply. However, experience from an earlier analysis of the ITS architecture [4] helped us forward.

Of the 14 vulnerabilities identified, we found countermeasures that directly address twelve of them. The last two, VU6 and VU7, are related to software bugs. Firewalls and link layer encryption may to some extent address these two by removing traffic from unknown sources. However, malicious traffic from known sources might still be received.

Addressing security in the repair shop network by using link layer encryption comes with some possibilities, but also with some drawbacks. The introduction of encryption at the link layer offers a basic protection level that the rest of the security mechanisms can be built on. The encryption keys used at the link layer can be used for mutual authentication of the connecting device and the DHCP service. Only authenticated devices can thereby retrieve an IP-address together with necessary information about the network, e.g., information about routing and DNS. Furthermore, link layer encryption will provide protection against eavesdropping for all upper layer protocols. This approach may also be used in other places, where LANs are used, e.g., in homes or in suppliers' networks. Unfortunately, encryption is not part of the common link layer protocols of today and such protocols need to be developed. We know of at least one such approach that has already been demonstrated in the Linux operating system [26]; still it needs to be investigated how such an approach will work in our context and how key management for vehicles and repair shops should be addressed. The main advantage of such a protocol would be that network and data authentication, data confidentiality, and data integrity are combined at the link layer. The network and data authentication will not be based on a specific communication technology, and data confidentiality and data integrity will be provided for all upper layer protocols at the same time.

In this work, we have addressed vehicle diagnostics within the repair shop, i.e., within a LAN, but the identified countermeasures may also be used when performing remote diagnostics outside the LAN.

Regarding authentication keys, we found that the loss of those used by diagnostics equipment is a major security problem. Authentications keys should therefore not give access to vehicles unless some authorisation mechanism also approves the access. Such authorisation can be given by the vehicle's owner or by issuing short-lived authentication keys to the diagnostics equipment. How authentication keys should be handled, especially for diagnostics equipment, needs careful considerations and it is important that possible approaches are identified soon.

XI. Conclusion

The evolution of a connected car is still just beginning and there are many security problems that need to be solved. In this paper, we have analysed the security of diagnostics services in connected repair shops. This has been done by applying a reduced version of the TVRA method. Even though we did not find the TVRA method easy to follow, the method was still useful. We have identified several security threats against the repair shop and the vehicles during service, and also suggested mechanisms to address these problems. To our big surprise, the biggest security threat was not related to the repair shop or the vehicles therein, but to other vehicles. If the keys used to authenticate repair shops to vehicles are stolen or copied, an attacker with access to these keys can create faked repair shop networks and vehicles connecting to them will be unable to differentiate these faked networks from real repair shop networks. Furthermore, our analysis suggests that addressing security at the link layer is a promising approach. This approach may integrate network authentication mechanisms during address allocation and also support encryption of data for all upper layer protocols with minimal modifications.

Acknowledgements

This research was funded by the project Security Framework for Vehicle Communication (2011-04434), co-funded by VINNOVA, the Swedish Governmental Agency for Innovation Systems.

References

[1] M. Shavit, A. Gryc, and R. Miucic. "Firmware Update Over The Air (FOTA) for Automotive Industry". In: *14th Asia Pacific Automotive Engineering Conference*. Hollywood, CA, USA, Aug. 2007. DOI: 10.4271/2007-01-3523.

[2] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. "Comprehensive Experimental Analyses of Automotive Attack Surfaces". In: *Proc. of the 20th USENIX Security Symposium*. San Francisco, CA, USA, Aug. 2011, pp. 77–92.

[3] *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis*. Tech. Spec. TS 102 165-1, v4.2.3. 650 Route des Locioles, F-06921 Sophia Antipolis Cedex, France: ETSI, Mar. 2011.

[4] *Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)*. Tech. Rep. TR 102 893, v1.1.1. 650 Route des Locioles, F-06921 Sophia Antipolis Cedex, France: ETSI, Mar. 2010.

[5] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil. "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions". In: *IEEE Communications Surveys & Tutorials* 13.4 (2011), pp. 584–616. DOI: 10.1109/SURV.2011.061411.00019.

[6] *Secure Vehicle Communication (SeVeCOM)*. URL: http://www.sevecom.org/ (visited on 07/25/2012).

[7] *E-safety Vehicle Intrusion Protected Applications (EVITA)*. URL: http://www.evita-project.org/ (visited on 07/25/2012).

[8] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux. "Secure Vehicular Communication Systems: Design and Architecture". In: *IEEE Communications Magazine* 46.11 (Nov. 2008), pp. 100–109. DOI: 10.1109/MCOM.2008.4689252.

[9] B. Oehry, C. van Driel, L. Haas, M. Wedlock, K. Perret, and T. van de Ven. *ITS Action Plan; Final Report Action 4.1*. Final Report. DG MOVE, Unit B4, Rue De Mot 28, 4/73. B-1049 Brussels, Belgium: European Commission, Dec. 2010.

[10] *Intelligent Transport Systems (ITS); Communications Architecture*. European Standard EN 302 665, v1.1.1. 650 Route des Locioles, F-06921 Sophia Antipolis Cedex, France: ETSI, Sept. 2010.

[11] *Intelligent Transport Systems (ITS); Security; Security Services and Architecture*. Tech. Spec. TS 102 731, v1.1.1. 650 Route des Locioles, F-06921 Sophia Antipolis Cedex, France: ETSI, Sept. 2010.

 ISBN: 978-1-61208-231-8

[12] *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions*. Tech. Rep. TR 102 638, v1.1.1. 650 Route des Locioles, F-06921 Sophia Antipolis Cedex, France: ETSI, June 2009.

[13] S. M. Mahmud, S. Shanker, and I. Hossain. "Secure Software Upload in an Intelligent Vehicle via Wireless Communication Links". In: *Proc. of the IEEE Intelligent Vehicles Symposium*. 2005, pp. 588–593. DOI: 10.1109/IVS.2005.1505167.

[14] I. Hossain and S. M. Mahmud. "Secure Multicast Protocol for Remote Software Upload in Intelligent Vehicles". In: *Proc. of the 5th Ann. Intel. Vehicle Systems Symp. of National Defense Industries Association (NDIA)*. National Automotive Center and Vectronics Technology. Traverse City, MI, June 2005, pp. 145–155.

[15] D. K. Nilsson and U. E. Larson. "Secure Firmware Updates over the Air in Intelligent Vehicles". In: *Proc. IEEE International Conference on Communications Workshops (ICC Workshops '08)*. May 2008, pp. 380–384. DOI: 10.1109/ICCW.2008.78.

[16] D. Nilsson, L. Sun, and T. Nakajima. "A Framework for Self-Verification of Firmware Updates over the Air in Vehicle ECUs". In: *GLOBECOM Workshops*. IEEE. Nov. 2008, pp. 1–5. DOI: 10.1109/GLOCOMW.2008.ECP.56.

[17] A. Weimerskirch. "Secure Software Flashing". In: *SAE Int. J. Passeng. Cars - Electron. Electr. Syst.* Vol. 2. 1. 2009, pp. 83–86.

[18] M. Idrees, H. Schweppe, Y. Roudier, M. Wolf, D. Scheuermann, and O. Henniger. "Secure Automotive On-Board Protocols: A Case of Over-the-Air Firmware Updates". In: *Communication Technologies for Vehicles*. Vol. 6596. LNCS. 2011, pp. 224–238. ISBN: 978-3-642-19785-7. DOI: 10.1007/978-3-642-19786-4_20.

[19] D. K. Nilsson, U. E. Larson, and E. Jonsson. "Creating a Secure Infrastructure for Wireless Diagnostics and Software Updates in Vehicles". In: *Proc. of the 27th International Conference on Computer Safety, Reliability, and Security (SAFECOMP '08)*. Newcastle upon Tyne, UK, 2008, pp. 207–220. ISBN: 978-3-540-87697-7. DOI: 10.1007/978-3-540-87698-4_19.

[20] *ISO/DIS 13400-1: Road vehicles — Diagnostic communication over Internet Protocol (DoIP) — Part 1: General information and use case definition*. ISO.

[21] M. Johanson, P. Dahle, and A. Söderberg. "Remote Vehicle Diagnostics over the Internet using the DoIP Protocol". In: *Proc. of the Sixth International Conference on Systems and Networks Communications (ICSNC 2011)*. IARIA. Barcelona, Spain, Oct. 2011, pp. 226–231.

[22] P. Kleberger, A. Javaheri, T. Olovsson, and E. Jonsson. "A Framework for Assessing the Security of the Connected Car Infrastructure". In: *Proc. of the Sixth International Conference on Systems and Networks Communications (ICSNC 2011)*. IARIA. Barcelona, Spain, Oct. 2011, pp. 236–241.

[23] R. Droms. "RFC 2131: Dynamic Host Configuration Protocol". Mar. 1997.

[24] *ISO/DIS 13400-2: Road vehicles — Diagnostic communication over Internet Protocol (DoIP) — Part 2: Network and transport layer requirements and services*. ISO.

[25] S. HomChaudhuri and M. Foschiano. "RFC 5517: Cisco Systems' Private VLANs: Scalable Security in a Multi-Client Environment". Feb. 2010.

[26] Y. Jerschow, C. Lochert, B. Scheuermann, and M. Mauve. "CLL: A Cryptographic Link Layer for Local Area Networks". In: *Security and Cryptography for Networks*. Vol. 5229. LNCS. 2008, pp. 21–38. ISBN: 978-3-540-85854-6. DOI: 10.1007/978-3-540-85855-3_3.

[27] F. Dressler, F. Kargl, J. Ott, O. Tonguz, and L. Wischhof. "Research Challenges in Intervehicular Communication: Lessons of the 2010 Dagstuhl Seminar". In: *IEEE Communications Magazine* 49.5 (May 2011), pp. 158–164. ISSN: 0163-6804. DOI: 10.1109/MCOM.2011.5762813.

[28] B. Issac. "Secure ARP and Secure DHCP Protocols to Mitigate Security Attacks". In: *International Journal of Network Security* 8.2 (2009), pp. 107–118.

APPENDIX A
THREAT AND VULNERABILITY ANALYSIS

In this appendix, the detailed results of the threat and vulnerability analysis are presented.

A model of the network with devices and possible communication paths for the analysis is shown in Figure 4. We identified 14 vulnerabilities which were classified based on the five threat categories defined by the TVRA method [3]: eavesdropping, unauthorised access, masquerade, forgery, and information corruption. The results are presented in Table III and the format is based on those used in [3, 4].

A few columns in Table III need to be explained. The *attack interface* identifies the communication interface where the vulnerability exists. The *source* is from where the vulnerability can be utilised. The source can be one of the following three:

- *radio.* A device only within the radio range of the repair shop.
- *local.* A device that is connected to, or within the radio range of, the repair shop network.
- *all.* Any host in the Internet, or any of the other two sources, radio and local.

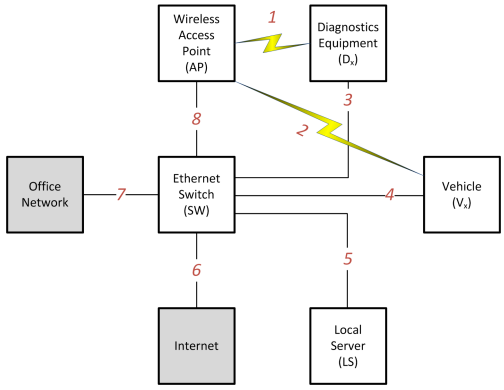


Figure 4. Assets in the repair shop. Physical assets are marked as white boxes.

Table III
VULNERABILITIES

ID	Threat Category	Weakness	Threat Agent	Unwanted Outcome	V cu ti
VU1	eavesdropping	weak protection of confidential diagnostics data and ECU firmware	device eavesdrop on network traffic	disclosure of confidential data	O
VU2	unauthorised access	weak authentication	someone tries to circumvent authentication mechanisms	disclosure of confidential data	O
VU3				manipulation of data	O
VU4		lack of proper protection of wireless connections	someone tries to circumvent protection mechanisms to establish a wireless connection	unauthorised devices get access to the repair shop network	O
VU5		lack of traffic separation	device communicates with the wrong device in the network	communication scenarios are violated, facilitating other attacks	O
VU6		software bugs	someone utilizes bugs to install malware	disclosure of confidential data	O
VU7				manipulation of data	O
VU8	masquerade	lack of proper device identification	device identifies itself as another entity (impersonation)	disclosure of confidential data	O
VU9				manipulation of data	O
VU10	forgery	lack of data authentication	someone injects fabricated diagnostics data into diagnostics session	final destination stores or processes malicious diagnostics data	O
VU11		weak integrity check of diagnostics data			O
VU12		lack of freshness in diagnostics session	someone replays a previously eavesdropped diagnostics session	a previous diagnostics session is executed	O
VU13		weak integrity check of vehicle ID broadcast	someone fabricates that a non-existing vehicle has arrived to the repair shop	diagnostics equipment establishes a diagnostics session to the wrong vehicle	O
VU14	information corruption	weak integrity check of diagnostics data	device modifies data during transmission	final destination stores or processes malicious diagnostics data, which could lead to other vulnerabilities, e.g., denial of service or buffer overflow.	O

 ISBN: 978-1-61208-231-8

Combined Histogram-based Features of DCT Coefficients in Low-frequency Domains for Face Recognition

Qiu Chen, Koji Kotani*, Feifei Lee, and Tadahiro Ohmi

New Industry Creation Hatchery Center, Tohoku University
** Department of Electronics, Graduate School of Engineering, Tohoku University*
Aza-Aoba 6-6-10, Aramaki, Aoba-ku, Sendai 980-8579, JAPAN
e-mail: qiu@fff.niche.tohoku.ac.jp

***Abstract*—Previously, We proposed an efficient algorithm using vector quantization (VQ) histogram for facial image recognition in low-frequency DCT domains. It can be considered that this algorithm is essential for utilizing the phase information of DCT coefficients by applying binary quantization on the DCT coefficient blocks. In this paper, we newly utilize energy histogram so as to add magnitude information of DCT coefficients. These two histograms, which contain both phase and magnitude information of a DCT transformed facial image, are utilized as a very effective personal value. Publicly available AT&T database is used for the evaluation of our proposed algorithm, which is consisted of 40 subjects with 10 images per subject containing variations in lighting, posing, and expressions. It is demonstrated that face recognition using combined histogram-based features of DCT coefficients in low frequency domains can achieve much higher recognition rate.**

Keywords-Face recognition; Vector quantizaiton (VQ); Energy histogram; DCT coefficients.

I. INTRODUCTION

Face recognition has been hot research topic for two decades due to its potential applications in many fields such as law enforcement applications, security applications and video indexing, etc. Many algorithms have been proposed for solving face recognition problem [1]-[11]. These algorithms can be roughly divided to two categories, namely, statistics-based and structure-based approaches. Statistics-based approaches [5], [6], [7] attempt to capture and define the face as a whole. The face is treated as a two dimensional pattern of intensity variation. Under this approach, the face is matched through finding its underlying statistical regularities. Based on the use of the Karhunen-Loeve transform, PCA [5] is used to represent a face in terms of an optimal coordinate system which contains the most significant eigenfaces and the mean square error is minimal. However, it is highly complicated and computational-power hungry, making it difficult to implement them into real-time face recognition applications. Structure-based approach [3], [4] uses the relationship between facial features, such as the locations of eye, mouth and nose. It can implement very fast, but recognition rate usually depends on the location accuracy of facial features, so it cannot give a satisfied recognition result. There are many other algorithms have been used for face recognition, such as Local Feature Analysis (LFA) [11], neural network [1], local autocorrelations and multi-scale integration technique [2], and other techniques have been proposed.

Discrete Cosine Transform (DCT) is not only widely used in many image and video compression standards [12], but also for pattern recognition as a means of feature extraction [13]-[21]. The main merit of the DCT is its relationship to the KLT [18]. It has been demonstrated that DCT best approach KLT [23], but DCT can be computationally more efficient than the KLT depending on the size of the KLT basis set.

In our previous work [27], we present a simple, yet highly reliable face recognition algorithm using vector quantization (VQ) method for facial image recognition in compressed DCT domain. Feature vectors of facial image are firstly generated by using DCT coefficients in low frequency domains. Then codevector referred count histogram, which is utilized as a very effective facial feature value, is obtained by VQ processing.

This algorithm can be considered utilizing the phase information of DCT coefficients by applying binary quantization on the DCT coefficient blocks. If we could add magnitude information of DCT coefficients, the composite features of face are expected to be more robust and effective. In this paper, we utilize energy histogram to represent magnitude features of DCT coefficients. These two histograms, which contain both phase and magnitude information of a DCT transformed facial image, are utilized as a very effective personal value. Recognition results with different type of histogram features are first obtained separately and then combined by weighted averaging.

This paper is organized as follows. A brief introduction to DCT as well as energy histogram is given in Section II. Our proposed face recognition method will be described in detail in Section III. Experimental results will be discussed in Section IV. Finally, we make a conclusion in Section V.

II. RELATED WORKS

A. Discrete Cosine Transform (DCT)

Discrete Cosine Transform (DCT) is used in JPEG compression standard. The DCT transforms spatial

 ISBN: 978-1-61208-231-8

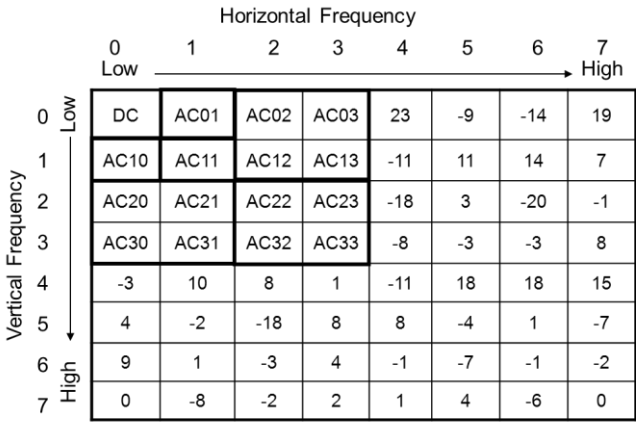


Figure 1. Generation of Low-frequency DCT coefficients (used as phase information)

information to decoupled frequency information in the form of DCT coefficients.

2D DCT with block size of N × N is defined as follows:

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cdot\cos(\frac{(2x+1)u\pi}{2N})\cos(\frac{(2y+1)v\pi}{2N}) \quad (1)$$

$$f(x,y) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1}\alpha(u)\alpha(v)C(u,v)\cdot\cos(\frac{(2x+1)u\pi}{2N})\cos(\frac{(2y+1)v\pi}{2N}) \quad (2)$$

$$\text{where, } \alpha(\omega) = \begin{cases} \frac{1}{\sqrt{N}} & : \quad for \quad \omega = 0 \\ \frac{2}{\sqrt{N}} & : \quad for \quad \omega = 1,2,...,N-1 \end{cases} \quad (3)$$

B. Face recognition using Binary vector quantization in low-frequency DCT domains

In our previous work [27], we proposed a feature extraction algorithm for face recognition using binary vector quantization (VQ) to generate feature vectors of facial image from DCT (Discrete Cosine transform) coefficients in low frequency domains.

First, low-pass filtering is carried out using 2-D moving filter. Block segmentation step, in which facial image is divided into small image blocks with an overlap, namely, by sliding dividing-partition one pixel by one pixel, is the following. Then the pixels in the image blocks (typical size is 8x8) are transformed using DCT according to the equation (1).

A typical sample of transformed block is shown in Figure 1. The DCT coefficients of the image block are then used to form a feature vector. From left to right and top to bottom, the frequency of coefficients changes from low to high as shown in Figure 1. Because low frequency component is more effective for recognition, we only use the coefficients on the left and above to extract features. The equation for calculation is shown below.

$$\begin{aligned} &a[0] = AC01; \\ &a[1] = AC11; \\ &a[2] = AC10; \\ &a[3] = (AC02 + AC03 + AC12 + AC13) / 4; \\ &a[4] = (AC22 + AC23 + AC32 + AC33) / 4; \\ &a[5] = (AC20 + AC21 + AC30 + AC31) / 4 \end{aligned} \quad (4)$$

where a[i] is the element of extracted feature vector, and d[i][j] is the coefficient value at point (*i*, *j*), respectively.

After that, quantization of the feature vectors is implemented. There are only 2 types of value for each a[i], so the number of combination of 6-dimensional vector is 64, which is very easy and fast to be determined. The number of vectors with same index number is counted and feature vector histogram is easily generated, and it is used as histogram feature of the facial image. In the registration procedure, this histogram is saved in a database as personal identification information. In the recognition procedure, the histogram made from an input facial image is compared with registered individual histograms and the best match is output as recognition result.

C. Energy histogram

A color histogram is obtained by counting the number of times a color occurs in an image. Similar to a color histogram, an energy histogram of the DCT coefficients is created by counting the number of times an energy level appears in a DCT blocks set of a DCT compressed image. An energy histogram (h_c) [30] of an 8x8 DCT block for a particular color component can be written as:

$$h_C[m] = \sum_{u=0}^{7}\sum_{v=0}^{7}\begin{cases}1 & if\ Q(F[u,v])=m \\ 0 & otherwise\end{cases} \quad (5)$$

with *Q(F[u,v])* denotes the dequantized coefficient's energy level at the *u*,*v* location.

Energy histogram has been used in image retrieval in [30], and also reported to be used for face recognition algorithm [31].

III. PROPOSED METHOD

As described in Section II (B), we have proposed a face recognition algorithm by applying binary quantization on the low-frequency DCT coefficient blocks, which was demonstrated to be effective for face recognition by experimental results. Actually, it can be thought that phase information of low-frequency DCT coefficients is extracted by this algorithm. If we could add magnitude information of DCT coefficients, the composite features of face are expected to be more robust and effective.

We utilize energy histogram to represent magnitude features of DCT coefficients. In this paper, we propose an

 ISBN: 978-1-61208-231-8

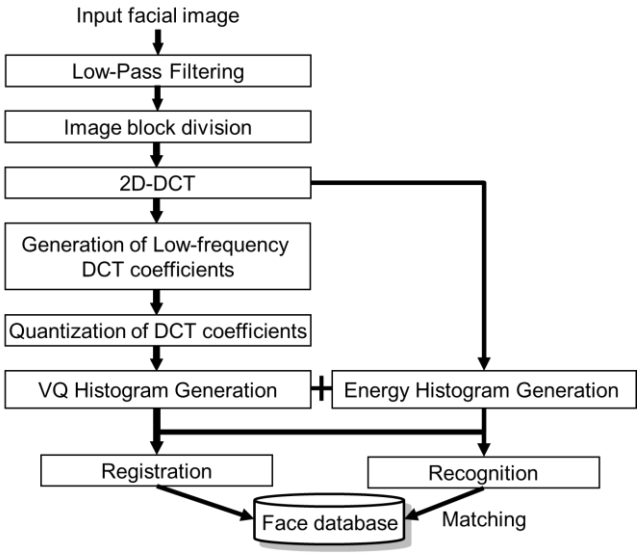


Figure 2. Face recognition process using combined histogram-based features.

Horizontal Frequency

Vertical Frequency	0 (Low)	1	2	3	4	5	6	7 (High)
0 (Low)	DC	AC01	AC02	AC03	23	-9	-14	19
1	AC10	AC11	AC12	AC13	-11	11	14	7
2	AC20	AC21	AC22	AC23	-18	3	-20	-1
3	AC30	AC31	AC32	AC33	-8	-3	-3	8
4	-3	10	8	1	-11	18	18	15
5	4	-2	-18	8	8	-4	1	-7
6	9	1	-3	4	-1	-7	-1	-2
7 (High)	0	-8	-2	2	1	4	-6	0

Figure 3. Low-frequency DCT coefficients for energy histogram.

improved face recognition algorithm using combined histogram-based features. Figure 2 shows proposed face recognition process steps. First, low-pass filtering is carried out using 2-D moving filter. This low-pass filtering is essential for reducing high-frequency noise and extracting most effective low frequency component for recognition.

Block segmentation step, in which facial image is divided into small image blocks with an overlap, namely, by sliding dividing-partition one pixel by one pixel, is the following. Then the pixels in the image blocks (typical size is 8x8) are transformed using DCT according to the equation (1). After generations of low-frequency DCT coefficients, binary quantization of the feature vectors is implemented as described in Section II (B), and then VQ histogram of low-frequency DCT coefficients is created.

On the other hand, energy histogram of low-frequency DCT coefficients is also generated after 2D-DCT. Because low frequency component is more effective for recognition, we only use the coefficients on the left and above to extract features. This can also reduce computation time compared with using the whole DCT coefficients. In this paper, we use 4x4 coefficient blocks as shown in Figure 3, the same domain as VQ histogram used at the upper left corner of the DCT coefficient block which retain the higher energy level of the image. The DC coefficient is not included in the features to reduce the influence of the lighting conditions of the images. Once the features have been selected, the energy histogram is created by using formula (5).

These two histograms, which contain both phase and magnitude information of a DCT transformed facial image, are utilized as a very effective personal value. Recognition results with different type of histogram features are first obtained separately and then combined by weighted averaging.

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

A. ORL database

Face database of AT&T Laboratories Cambridge [25], [26] is used for recognition experiments. In the database, 10 facial images for each of 40 persons (totally 400 images) with variations in face angles, face sizes, facial expressions, and lighting conditions are included. Each image has a resolution of 92x112. Five images were selected from each person's 10 images as probe images and remaining five images are registered as album images. Recognition experiment is carried out for 252 ($_{10}C_5$) probe-album combinations by rotation method. The algorithm is programmed by ANSI C and run on PC (Pentium(R)D processor 840 3.2GHz).

B. Results and discussions

In our experiments, the bin size of energy histogram is set to 100. Figure 4 shows the comparison of the recognition results with different features. The average recognition rates obtained by each case with block size of 8x8 are shown here. Recognition success rates are shown as a function of filter size. Although recognition results only using energy histogram of low-frequency DCT coefficients ("N8_energy_hist") are not satisfied, average recognition rate increases combined with VQ histogram of low-frequency DCT coefficients ("N8_combined"). The maximum of the average rate 95.4% is achieved, which is 1.7% higher than that only using VQ histogram in our previous work ("N8_VQ_hist", the maximum of the average rate is 93.7%) [27].

Figure 5 shows recognition results using combined features with the same weighting coefficient of two

 ISBN: 978-1-61208-231-8

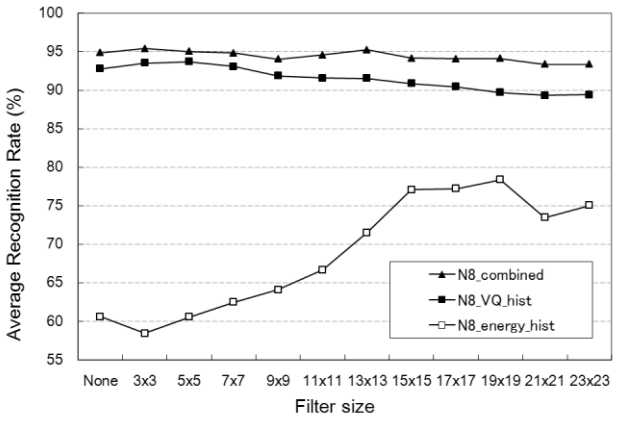


Figure 4. Comparison of recognition results

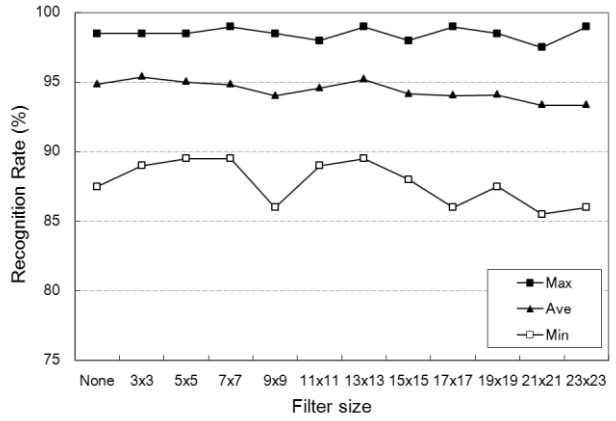


Figure 5. Recognition rate as a function of filter size (image block size is 8x8 here)

histogram features. Recognition success rates are shown as a function of filter size. "Max," "Min" and "Ave" stand for the best case, worst case, and average results in 252 ($_{10}C_5$) probe-album combinations, respectively. The highest average recognition rate of 95.38% is obtained at the filter size of 3x3. Low pass filter is effective for eliminating noise component and extracting important frequency component for recognition.

By combining these two different features, namely phase information and magnitude information of low-frequency DCT coefficient blocks, the most important information for face recognition can effectively be extracted.

V. CONCLUSIONS AND FUTURE WORK

We have developed a very simple yet highly reliable face recognition method using features extracted from low-frequency DCT domain, which is combined with VQ histogram and energy histogram. Excellent face recognition performance has been verified by using publicly available ORL database. The effect of the image block size will be discussed in our future work, as well as the performance evaluation of the face recognition using larger face database.

ACKNOWLEDGMENT

This research was partially supported by research grant from Support Center for Advanced Telecommunications Technology Research, Foundation (SCAT).

REFERENCES

[1] R. Chellappa, C. L. Wilson, and S. Sirohey, "Human and machine recognition of faces: a survey," Proc. of IEEE, vol. 83, no. 5, 1995, pp.705-740.

[2] S. Z. Li and A. K. Jain, "Handbook of face recognition," Springer, New York, 2005.

[3] R. Brunelli and T. Poggio, "Face recognition: features versus templates," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 15, no. 10, 1993, pp. 1042-1052.

[4] L. Wiskott, J. M. Fellous, N. Kruger, and C. Malsburg, "Face recognition by elastic bunch graph matching," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 19, no. 10, 1997, pp.775-780.

[5] M. Turk and A. Pentland, "Eigenfaces for recognition," Journal of Cognitive Neuroscience, vol. 3, no. 1, 1991, pp. 71-86.

[6] W. Zhao, "Discriminant component analysis for face recognition," Proc. ICPR'00, Track 2, 2000, pp. 822-825.

[7] K.M. Lam, H. Yan, "An analytic-to-holistic approach for face recognition based on a single frontal view," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 20, no. 7, 1998, pp. 673-686.

[8] M. S. Bartlett, J. R. Movellan, and T. J. Sejnowski, "Face recognition by independent component analysis," IEEE Trans. on Neural Networks, vol. 13, no. 6, 2002, pp. 1450-1464.

[9] B. Moghaddam and A. Pentland, "Probabilistic visual learning for object representation," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 19, no. 7, 1997, pp. 696-710.

[10] S. G. Karungaru, M. Fukumi, and N. Akamatsu, "Face recognition in colour images using neural networks and genetic algorithms," Int'l Journal of Computational Intelligence and Applications, vol. 5, no. 1, 2005, pp. 55-67.

[11] P. S. Penev and J. J. Atick, "Local feature analysis: a general statistical theory for object representation," Network: Computation in Neural Systems, vol. 7, no. 3, 1996, pp. 477-500.

[12] W. B. Pennebaker and J. L. Mitchell, "JPEG still image data compression standard," Van Nostrand Reinhold, New York, 1993.

[13] H. B. Kekre, T. K. Sarode, P. J. Natu, and S. J. Natu, "Transform based face recognition with partial and full feature vector using DCT and Walsh transform," Proc. of the Int'l Conf. & Workshop on Emerging Trends in Technology, 2011, pp. 1295-1300.

[14] Z. Liu and C. Liu, "Fusion of color, local spatial and global frequency information for face recognition," Pattern Recognition, vol. 43, Issue 8, Aug. 2010, pp. 2882-2890.

[15] H. F. Liau, K. P. Seng, L. M. Ang, and S. W. Chin, "New parallel models for face recognition," Recent Advances in Face Recognition, Edited by K. Delac etc., InTech, 2008.

[16] R. Tjahyadi, W. Liu, S. An and S. Venkatesh, "Face recognition via the overlapping energy histogram," Int'l Joint Conf. on Artificial Intelligence, 2007, pp. 2891-2896.

 ISBN: 978-1-61208-231-8

[17] D. Zhong and I. Defee, "Pattern recognition in compressed DCT domain," Proc. of Int'l Conf. on Image Processing, vol. 3, 2004, pp. 2031 - 2034.

[18] Z. M. Hafed and M. D. Levine, "Face recognition using the Discrete Cosine Transform," Int'l Journal of Computer Vision, vol. 43, no. 3, 2001, pp. 167-188.

[19] S. Eickeler, S. Müller and G. Rigoll, "Recognition of JPEG compressed face images based on statistical methods," Image and Vision Computing Journal, Special Issue on Facial Image Analysis, vol. 18, no. 4, Mar. 2000, pp. 279-287.

[20] S. Eickeler, S. Müller and G. Rigoll, "High quality face recognition in JPEG compressed images," Proceeding of Int'l Conf. on Image Processing, vol. 1, Oct. 1999, pp. 672-676.

[21] V. Nefian and M. H. Hayes, "Hidden Markov models for face recognition," Int'l Conf. on Acoustics, Speech, and Signal Processing, May 1998, pp. 2721-2724.

[22] M. Shneier and M Abdel-Mottaleb, "Exploiting the JPEG compression scheme for image retrieval," IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 18, no. 8, Aug. 1996.

[23] A. Jain, Fundamentals of Digital Image Processing, Prentice: Englewood Cliffs, NJ, 1989.

[24] A. Gersho and R. M. Gray, "Vector quantization and signal compression," Kluwer Academic, 1992.

[25] AT&T Laboratories Cambridge, "The database of faces," at http://www.cl.cam.ac.uk/research/dtg/attarchive/ facedatabase. html.

[26] F. Samaria and A. Harter, "Parameterisation of a stochastic model for human face identification," 2nd IEEE Workshop on Applications of Computer Vision, 1994, pp. 138-142.

[27] Q. Chen, K. Kotani, F. F. Lee, and T. Ohmi, "Face recognition using VQ Histogram in compressed DCT domain," Journal of Convergence Information Technology, vol. 7, no. 1, 2012, pp. 395-404.

[28] K. Kotani, Q. Chen, F. F. Lee, and T. Ohmi "Region-division VQ histogram method for human face recognition," Intelligent Automation and Soft Computing, vol. 12, no. 3, 2006, pp. 257-268.

[29] P. J. Phillips, H. Wechsler, J. Huang, and P. Rauss, "The FERET database and evaluation procedure for face recognition algorithms," Image and Vision Computing J, vol. 16, no. 5, 1998, pp. 295-306.

[30] J. A. Lay and L. Guan, "Image Retrieval based on energy histogram of the low frequency DCT coefficients," IEEE Int'l Conf. on Acoustics Speech and Signal Processing, vol. 6, 1999, pp. 3009-3012.

[31] R. Tjahayadi, W. Liu, and S. Venkatesh, "Application of the DCT energy histogram for face recognition," Proc. of 2nd Int'l conf. on Information Technology for Application (ICITA), Sydney, 2004, pp. 314-319.

 ISBN: 978-1-61208-231-8

Face Recognition Algorithm Using Muti-direction Markov Stationary Features and Adjacent Pixel Intensity Difference Quantization Histogram

Feifei Lee, Koji Kotani*, Qiu Chen, and Tadahiro Ohmi

New Industry Creation Hatchery Center, Tohoku University
** Department of Electronics, Graduate School of Engineering, Tohoku University*
Aza-Aoba 6-6-10, Aramaki, Aoba-ku, Sendai 980-8579, JAPAN
e-mail: fei@fff.niche.tohoku.ac.jp

***Abstract*—We have proposed a robust face recognition algorithm using adjacent pixel intensity difference quantization (APIDQ) histogram combined with Markov Stationary Features (MSF) so as to add spatial structure information to histogram features in our previous work. We named the new histogram feature as MSF-DQ feature. In this paper, we extend original MSF to multi-direction MSF by generating co-occurrence matrices with orientations of 0, 45, 90, 135 degrees, and then extract corresponding MSF-DQ features for every direction. Publicly available AT&T database of 40 subjects with 10 images per subject containing variations in lighting, posing, and expressions, is used to evaluate the performance of the proposed algorithm. Experimental results show face recognition using proposed multi-direction MSF-DQ features is more efficient compared with the original algorithm.**

Keywords-Face recognition; Adjacent pixel intensity difference quantization (APIDQ); Markov stationary feature (MSF); Multi-direction; Histogram feature.

I. INTRODUCTION

As a more natural and effective person identification method compared with that using other biometric features such as voice, fingerprint, iris pattern, etc., a lot of face recognition algorithms have been proposed [1]-[14] in the last two decades. These algorithms can be mainly categorized into two groups, that is to say, structure-based and statistics-based.

In the structure-based approaches [3][4], recognition is based on the relationship between human facial features such as eye, mouth, nose, profile silhouettes and face boundary. Statistics-based approaches [5][6][7] attempt to capture and define the face as a whole. The face is treated as a two dimensional pattern of intensity variation. Under this approach, the face is matched through finding its underlying statistical regularities. Principal component analysis (PCA) is a typical statistics-based technique [5]. However, these techniques are highly complicated and are computationally power hungry, making it difficult to implement them into real-time face recognition applications.

In [18][19], a very simple, yet highly reliable face recognition method called Adjacent Pixel Intensity Difference Quantization (APIDQ) Histogram Method is proposed, which achieved the real-time face recognition. At each pixel location in an input image, a 2-D vector (composed of the horizontally adjacent pixel intensity difference (dIx) and the vertically adjacent difference (dIy)) contains information about the intensity variation angle (θ) and its amount (r). After the intensity variation vectors for all the pixels in an image are calculated and plotted in the r-θ plane, each vector is quantized in terms of its θ and r values. By counting the number of elements in each quantized area in the r-θ plane, a histogram can be created. This histogram, obtained by APIDQ for facial images, is utilized as a very effective personal feature. Experimental results show a recognition rate of 95.7 % for 400 images of 40 persons (10 images per person) from the publicly available AT&T face database [20].

Li et al. [19] proposed Markov stationary feature (MSF), which can encode the relationships of intra-bin and inter-bin into histograms. Motivated by this consideration, we combine the APIDQ histogram with Markov stationary feature (MSF), so as to encode spatial structure information within and between histogram bins [17][18]. The MSF extends the APIDQ histogram features by characterizing the spatial co-occurrence of histogram patterns using the Markov chain models and improves the distinguishable capability of APIDQ features to extra-bin distinguishable level [19]. Experimental results demonstrated that the algorithm using the MSF-DQ features is more robust for face recognition evaluated by using the publicly available database of AT&T [20].

Pixel pairs in all directions are counted to generate a single co-occurrence matrix in original MSF algorithm. Considering that the co-occurrence matrices have been widely used in as a feature in registration and segmentation problems [23][24][24], we extend original MSF to multi-direction MSF by generating co-occurrence matrices with orientations of 0, 45, 90, 135 degrees, and then extract corresponding MSF-DQ feature for each direction. Therefore, more comprehensive personal feature information can be obtained by using multi-direction MSF-DQ features, which is named MDMSF-DQ.

In Section II, we will first introduce Markov stationary feature (MSF) as well as the Adjacent Pixel Intensity Difference Quantization (APIDQ) histogram feature which had been successfully applied to face recognition previously, and then describe proposed face recognition algorithm using multi-direction MSF-DQ features (MDMSF-DQ) in Section

 ISBN: 978-1-61208-231-8

III. Experimental results will be discussed in Section IV. Finally, conclusions will be given in Section V.

II. RELATED WORKS

A. Markov Stationary features (MSF)

The Markov stationary feature (MSF) [19] extends the APIDQ histogram features by characterizing the spatial co-occurrence of histogram patterns using the Markov chain models and improves the distinguishable capability of APIDQ features to extra-bin distinguishable level. We will briefly introduce the MSF in this section.

Let p_k be a pixel in image I, the spatial co-occurrence matrix is defined as $C = (c_{ij})_{K\times K}$ where

$$c_{ij} = \#(p_1 = c_i, p_2 = c_j \| p_1 - p_2 | = d)/2, \quad (1)$$

in which d (d=1 in this paper) indicates L_1 distance between two pixels p_1 and p_2, and c_{ij} counts the number of spatial co-occurrence for bin c_i and c_j.

The co-occurrence matrix c_{ij} can be interpreted in a statistical view. Markov chain model is adopted to characterize the spatial relationship between histogram bins.

The bins are treated as states in Markov chain models, and the co-occurrence is viewed as the transition probability between bins. In this way, the MSF can transfer the comparison of two histograms to two corresponding Markov chains.

The elements of the transition matrix *P* are constructed from the spatial co-occurrence *C* by formula (2).

$$P_{ij} = c_{ij} / \sum_{j=1}^{K} c_{ij} \quad (2)$$

The state distribution after n steps is defined as $\pi(n)$, and the initial distribution is $\pi(0)$, the Markov transition matrix obeys following rules.

$$\pi(n+1) = \pi(n)P,\ \pi(n) = \pi(0)P^n; \quad (3)$$
$$P^{m+n} = P^m P^n$$

where $\pi(0)$ is defined as

$$\pi(0) = c_{ii} / \sum_{i=1}^{K} c_{ii} \quad (4)$$

According to the formula (3), we can get a distribution of π called a stationary distribution which satisfies

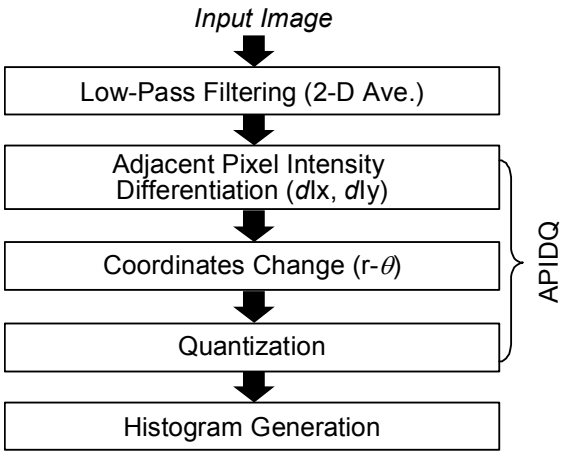


Figure 1. Processing steps of APIDQ histogram method.

$$\pi = \pi P \quad (5)$$

The stationary distribution becomes the final representation of MSF. Obtaining the MSF of each image, the comparison of two histograms is transferred to the comparison of two corresponding Markov chains.

B. Adjacent Pixel Intensity Difference Quantization (APIDQ)

The Adjacent Pixel Intensity Difference Quantization (APIDQ) histogram method [15] has been developed for face recognition previously. Figure 1 shows the processing steps of APIDQ histogram method. In APIDQ, for each pixel of an input image, the intensity difference of the horizontally adjacent pixels (*d*Ix) and the intensity difference of the vertically adjacent pixels (*d*Iy) are first calculated by using simple subtraction operations shown as formula (6).

$$dIx(i,j) = I(i+1,j) - I(i,j)$$
$$dIy(i,j) = I(i,j+1) - I(i,j) \quad (6)$$

A calculated (*dIx*, *dIy*) pair represents a single vector in the *dIx*-*dIy* plane. By changing the coordinate system from orthogonal coordinates to polar coordinates, the angle θ and the distance *r* represent the direction and the amount of intensity variation, respectively. After processing all the pixels in an input image, the dots representing the vectors are distributed in the *dIx*-*dIy* plane. The distribution of dots (density and shape) represents the features of the input image.

Each intensity variation vector is then quantized in the r-θ plane. Quantization levels are typically set at 8 in θ-axis and 8 in *r*-axis (totally 50). Since *dIx*-*dIy* vectors are concentrated in small-r (small-*dIx*, -*dIy*) region, non-uniform quantization steps are applied in *r*-axis. The number

 ISBN: 978-1-61208-231-8

of vectors quantized in each quantization region is counted and a histogram is generated. In the face recognition approach, this histogram becomes the feature vector of the human face.

The essence of the APIDQ histogram method can be considered that the operation detects and quantizes the direction and the amount of intensity variation in the image block. Hence the APIDQ histogram contains very effective image feature information. The MSF extends histogram based features with spatial structure information of images, and transfer the comparison of two histograms to two corresponding Markov chains.

III. PROPOSED FACE RECOGNITION ALGORITHM

A. Generation of 4 directions co-occurrence matrices

Pixel pairs in all directions are counted to generate a single co-occurrence matrix in original MSF algorithm. In this paper, we extend original MSF to multi-direction MSF by generating co-occurrence matrices with orientations of 0, 45, 90, 135 degrees as shown in Figure 2.

Because different MSF-DQ features are extracted with different direction co-occurrence matrices of the image, more comprehensive personal feature information can be obtained by combining multiple recognition results using 4 direction co-occurrence matrices.

In this paper, we employ 4 direction co-occurrence matrices for the facial image to extract more powerful personal feature. As shown in Figure 2, after APIDQ processing is carried out, MSF-DQ features at different directions are extracted from corresponding co-occurrence matrices. Recognition results are firstly obtained using MSF-DQ features at different directions separately and then combined by weighted averaging.

B. Proposed algorithm

The procedure of proposed face recognition algorithm using APIDQ histogram combined with MSF is shown in Figure 3. Low-pass filtering is first carried out before APIDQ using a simple 2-D moving average filter. This low-pass filtering is essential for reducing the high-frequency noise and extracting the most effective low frequency component for recognition. Then original APIDQ is implemented and quantization region number corresponding to each 2x2 image block is calculated. As shown in Figure 3, because each 2x2 image block can be regarded as a pixel of color c_i , the co-occurrence matrix for APIDQ can be computed according to formula (1). But instead of counting pixel pairs in all directions to generate a single co-occurrence matrix in original MSF algorithm, co-occurrence matrices at 4 different directions of 0, 45, 90, 135 degrees are generated.

The Markov transition matrix *P* for each direction of co-occurrence matrix is calculated by formula (2). Then the stationary distribution of corresponding direction can be approximated by the average of each row $\vec{a}_i$ of A_n using formula (7).

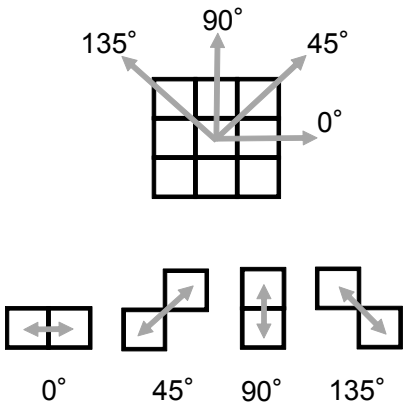


Figure 2. Extraction of Multi-direction pixel pairs .

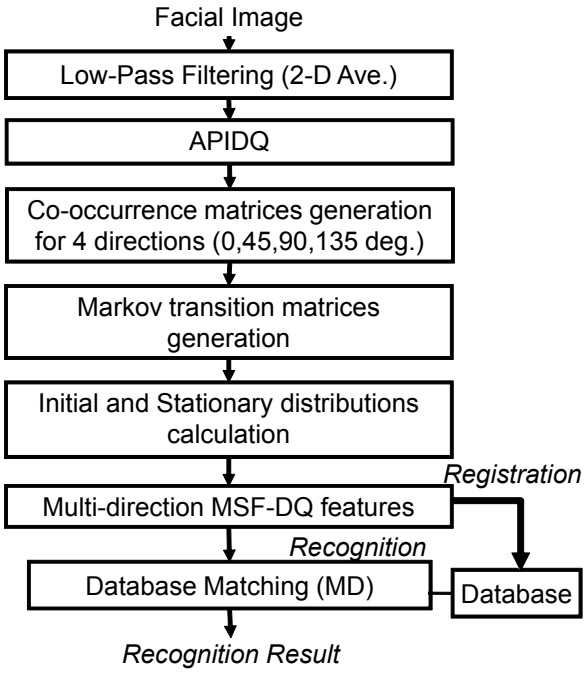


Figure 3. Proposed face recognition algorithm using multi-direction MSF-DQ features (MDMSF-DQ).

$$\pi \approx \frac{1}{K} / \sum_{i=1}^{K} \vec{a}_i \text{ , where } A_n = [\vec{a}_1, \cdots, \vec{a}_k]^T, \qquad (7)$$

$$A_n = \frac{1}{n+1}(I + P + P^2 + \cdots + P^n) \qquad (8)$$

n =50 is used as same as in [19]. The initial distribution $\pi(0)$ can be obtained by formula (4). As shown in formula (9), the Markov stationary feature in each direction is defined as the combination of the initial distribution $\pi(0)$ and the stationary distribution π after n steps.

$$\vec{h}_{MSF-DQ} = [\pi(0), \pi]^T \quad (9)$$

We call MSF extension of APIDQ histogram MSF-DQ feature. The MSF-DQ feature made from each direction is compared with those from the same direction in the database by calculating distances (d_i) between them using the same distance calculation formula as in [19]. Then the integrated distances (D) are obtained by weighted averaging as shown in the following formula (10).

$$D = \frac{\sum w_i d_i}{\sum w_i} \quad (10)$$

where w_i is weighting coefficient of the different directions, The best match is output as recognition result by searching the minimum integrated distance.

Figure 4. Samples of the database of AT&T Laboratories Cambridge.

IV. EXPERIMENTAL RESULTS AND DISCUSSIONS

A. Data sets

The publicly available face database of AT&T Laboratories Cambridge [20], [21]is used for the analysis and recognition experiments. Forty people with 10 facial images each, (totaling 400 images), with variations in face angles, facial expressions, and lighting conditions are included in the database. Each image has a resolution of 92x112. Figure 4 shows typical image samples of the database of AT&T Laboratories Cambridge. From the 10 images for each person, five were selected as probe images and the remaining five were registered as album images. Recognition experiments were carried out for 252 ($_{10}C_5$) probe-album combinations using the rotation method.

B. Experimental results

Comparison of recognition results are shown in Figure 5. Recognition success rates are shown as a function of filter size. The filter size represents the size of the averaging filter core. A size of F3, for instance, represents the filter using a 3x3 filter core. Figure 5 shows the comparison between the recognition results using different direction MSF-DQ features separately and multi-direction MSF-DQ features. Average recognition rate is shown here. "bin 50 (original DQ)" stands for the case that original APIDQ utilizes quantization table containing the number of bins of 50 in [15][16]. "bin50_all_directions" stands for the case using pixel pairs in all directions counted to generate a single co-occurrence matrix in original MSF algorithm. "bin50_0:1:0:1", "bin50_1:0:1:0", and "bin50_1:1:1:1", stand for the cases using combination of various direction MSF-DQ features of 0, 45, 90, 135 degrees respectively, which weighting coefficient at each direction level is set as 0 or 1.

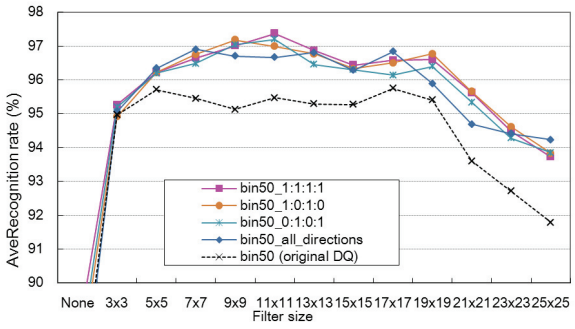


Figure 5. Comparison of results. Average recognition rate is shown here.

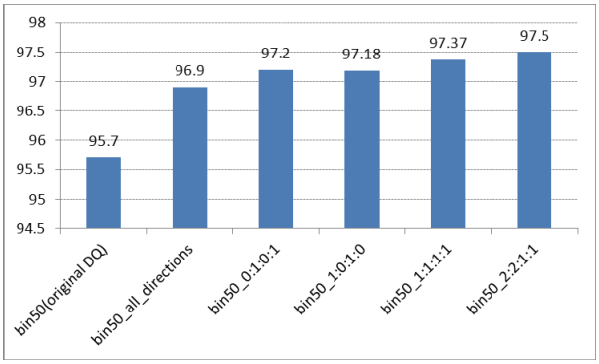


Figure 6. Comparison of results. Maximum average recognition rate is shown here.

The best performance of the average recognition rate 96.9% is obtained at original image size of 92x112 when using all-direction MSF-DQ features. By using multi-direction MSF-DQ features with the weighting coefficient at each direction level of 1, highest recognition rate increases to 97.37%. It can be said that multi-direction MSF-DQ features is more robust than original MSF-DQ features. We notice that the case that only using the combination of 0, 90 degrees or the combination of 45, 135 degrees can achieve similar recognition accuracy with that using 4 directions.

 ISBN: 978-1-61208-231-8

Figure 6 shows comparison results of the maximum average recognition rate using some combinations. Maximum of the average recognition rate 97.5% is achieved at the combination of weighting coefficients of 2:2:1:1 for 0, 45, 90, 135 degrees.

V. CONCLUSION AND FUTURE WORK

In this paper, we improved our face recognition using multi-direction MSF-DQ feature by generating co-occurrence matrices with orientations of 0, 45, 90, 135 degrees, and then extract corresponding MSF-DQ feature for each direction multi-direction for the facial image to extract more powerful personal feature. Excellent face recognition performance as large as a 97.5% recognition rate has been achieved by using the publicly available database of AT&T. It can be said that multi-direction MSF-DQ features is more is more robust for face recognition.

Because AT&T database is not a large face database, we will evaluate our proposed algorithm for practical application by using large database of FERET in our future work.

ACKNOWLEDGMENT

This research was partially supported by the Ministry of Education, Culture, Sports, Science and Technology of Japan, Grant-in-Aid for Scientific Research (C), No. 24500104, 2012-2015, and also by research grant from Support Center for Advanced Telecommunications Technology Research, Foundation (SCAT).

REFERENCES

[1] R. Chellappa, C. L. Wilson, and S. Sirohey, "Human and machine recognition of faces: a survey," Proc. IEEE, vol. 83, no. 5, 1995, pp.705-740.

[2] S. Z. Li and A. K. Jain, "Handbook of face recognition," Springer, New York, 2005.

[3] R. Brunelli and T. Poggio, "Face recognition: features versus templates," IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 15, no. 10, Oct. 1993, pp. 1042-1052.

[4] L. Wiskott, J. M. Fellous, N. Kruger, and C. Malsburg, "Face recognition by elastic bunch graph matching," IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 19, no. 10, 1997, pp. 775-780.

[5] M. Turk and A. Pentland, "Eigenfaces for recognition," Journal of Cognitive Neuroscience, vol. 3, no. 1, Mar. 1991, pp. 71-86.

[6] W. Zhao, "Discriminant component analysis for face recognition," Proc. in the Int'l Conf. on Pattern Recognition (ICPR'00), Track 2, 2000, pp. 822-825.

[7] K.M. Lam and H. Yan, "An analytic-to-holistic approach for face recognition based on a single frontal view," IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 20, no. 7, 1998, pp. 673-686.

[8] M.S. Bartlett, J.R. Movellan, and T.J. Sejnowski, "Face recognition by independent component analysis," IEEE Trans. on Neural Networks, vol. 13, no. 6, 2002, pp. 1450-1464.

[9] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, "Eigenface vs. Fisherfaces: Recognition using class specific linear projection," IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 19, May 1997, pp. 711-720.

[10] B. Moghaddam and A. Pentland, "Probabilistic visual learning for object representation," IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 19, no. 7, 1997, pp. 696-710.

[11] S. G. Karungaru, M. Fukumi, and N. Akamatsu, "Face recognition in colour images using neural networks and genetic algorithms," Int'l Journal of Computational Intelligence and Applications, vol. 5, no. 1, 2005, pp. 55-67.

[12] Z. Liu and C. Liu, "Fusion of color, local spatial and global frequency information for face recognition," Pattern Recognition, vol. 43, Issue 8, Aug. 2010, pp. 2882-2890.

[13] H. F. Liau, K. P. Seng, L. M. Ang, and S. W. Chin, "New parallel models for face recognition," Recent Advances in Face Recognition, Edited by K. Delac etc., InTech, 2008.

[14] Q. Chen, K. Kotani, F. F. Lee, and T. Ohmi, "Face recognition using VQ histogram in compressed DCT domain," Journal of Convergence Information Technology, vol. 7, no. 1, 2012, pp. 395-404.

[15] K. Kotani, F. F. Lee, Q. Chen, and T. Ohmi, "Face recognition based on the adjacent pixel intensity difference quantization histogram method," 2003 Int'l Symp. on Intelligent Signal Processing and Communication Systems, D7-4, 2003, pp. 877-880.

[16] F. F. Lee, K. Kotani, Q. Chen, and T. Ohmi, "Face recognition using adjacent pixel intensity difference quantization histogram," Int'l Journal of Computer Science & Network Security, vol. 9, no. 8, 2009, pp. 147-154.

[17] F. F. Lee, K. Kotani, Q. Chen, and T. Ohmi, "A robust face recognition algorithm using Markov stationary features and adjacent pixel intensity difference quantization histogram," Proc. in 7th Int'l Conf. on Signal Image Technology & Internet Based Systems (SITIS 2011), France, 2011, pp. 334-339.

[18] F. F. Lee, K. Kotani, Q. Chen, and T. Ohmi, "Face recognition using adjacent pixel intensity difference quantization histogram combined with Markov stationary features," Int'l Journal of Advancements in Computing Technology, vol. 4, no. 12, 2012, pp. 327-335.

[19] J. Li, W. Wu, T. Wang, and Y. Zhang, "One step beyond histograms: Image representation using Markov stationary features," Proc. in the IEEE Conf. on Computer Vision and Pattern Recognition (CVPR'08) , 2008, pp. 1-8.

[20] AT&T Laboratories Cambridge, The Database of Faces, at http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html.

[21] F. Samaria and A. Harter, "Parameterisation of a stochastic model for human face identification," 2nd IEEE Workshop on Applications of Computer Vision, 1994, pp. 138-142.

[22] P. J. Phillips, H. Wechsler, J. Huang, and P. Rauss, "The FERET database and evaluation procedure for face recognition algorithms," Image and Vision Computing J., vol. 16, no. 5, 1998, pp. 295-306.

[23] J. Malone, S. Prabhu, and P. Goddard, "The use of co-occurrence features in medical imaging: an empirical study," Visualization, Imaging, and Image Processing, 2005.

[24] S. Hentschel, F. Kruggel, "Segmentation of the intracranial compartment: a registration approach," Medical Imaging and Augmented Reality (Beijing), Lecture Notes in Computer Science vol. 3150, 2004, pp. 253-260.

[25] P. Maji, M.K. Kundu, and B. Chanda, "Segmentation of brain MR images using Fuzzy sets and modified co-occurrence matrix," IET Int'l Conf. on Visual Information Engineering (VIE 2006), Sep. 2006, pp. 327-332.

 ISBN: 978-1-61208-231-8

An ABAC-based Policy Framework for Dynamic Firewalling

Sören Berger*, Alexander Vensmer† and Sebastian Kiesel‡
*Computing Center
University of Stuttgart
Stuttgart, Germany
e-mail: soeren.berger@rus.uni-stuttgart.de
†Institute of Communication Networks
University of Stuttgart
Stuttgart, Germany
e-mail: alexander.vensmer@ikr.uni-stuttgart.de
‡Computing Center
University of Stuttgart
Stuttgart, Germany
e-mail: sebastian.kiesel@rus.uni-stuttgart.de

***Abstract*—This paper presents the Policy Framework of DynFire, a novel approach for attribute-based, dynamic control of network firewalls. DynFire allows an individually controlled, secure access to IT resources of a large organization, with particular focus on mobile users and users with restricted rights, such as subcontractors. The basic assumption behind DynFire is that, within a secured network domain separated from the Internet, a temporary binding between an IP address and a single user ID can be established. Users with different attributes can authenticate to the network and get individual access to network resources. To administrate such a large amount of users and different access rights within a secured network domain of an organization, which includes distributed organisational zones, a policy framework is needed. The following paper presents a policy framework for dynamic and distributed firewalls which is able to grant access control on a per-user basis, with multitenancy capabilities and administrative delegation.**

Keywords-dynamic firewall control; network security; policy based network access control.

I. Introduction

Firewalls are a well-understood and widely deployed means of protecting IP networks [1]. Their use is based on the assumption that the network can be divided into distinct domains with different security requirements and threat levels [2]. Located at domain boundaries, firewalls forward or reject network traffic between these domains, according to security policies that are usually configured statically into the firewalls [3]. However, this assumption, and thus the applicability of firewalls, is increasingly challenged. With the widespread use of mobile wireless as well as remote access over the Internet, domain borders get more and more blurred.

A mobile user changing from one access network to another, usually, receives a new IP address randomly chosen from an address pool. Therefore, IP packets, *usually*, do not carry enough information for a firewall to perform user-based access control decisions. While this puts the usefulness of firewalls into question, other developments reinforce the need for them. As the operator of a large campus network, we encounter an increasing number of devices in our network, which are not "classic" telecommunications or office PC equipment. This includes, e. g., building automation systems or scientific measurement devices. While these systems are often vulnerable due to missing or outdated security mechanisms (e. g., operating system updates, virus scanners, password policies, etc.), they also have an increased need for remote access, e. g., for maintenance technicians. Placing a firewall in front of such systems may improve security, but conventional firewalls with static policies are not flexible enough for fine-grained access control. Wide spread firewalls and distributed administration added new requirements to enterprise institutions firewall scenarios. This paper presents the Policy Framework of DynFire, a new framework for the

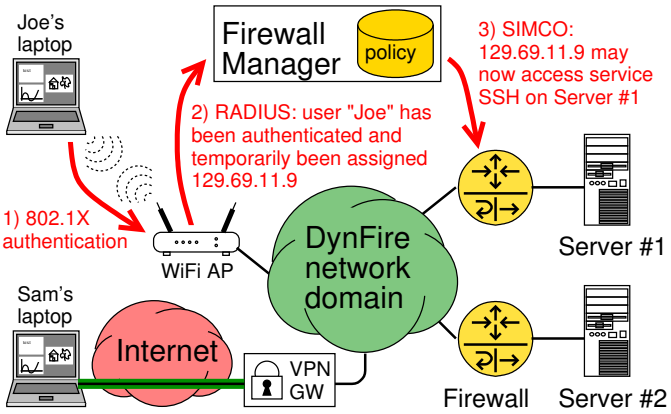


Figure 1. DynFire scenario

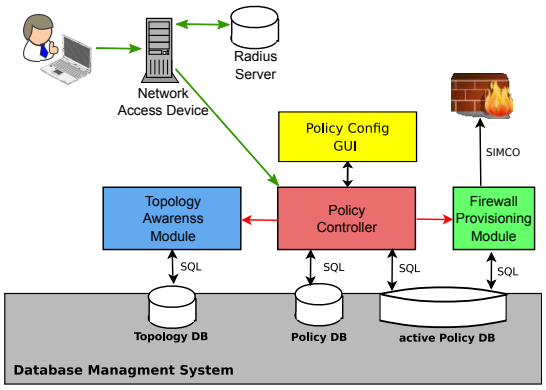


Figure 2. DynFire architecture

dynamic attribute-based configuration of firewalls. The rest of the paper is structured as follows. Section II describes the system architecture of DynFire. Section III present the Policy Framework. Section IV summarizes the related work. Section V concludes the paper and summarizes further steps.

II. DynFire System Architecture

The goal is to create a policy framework for the architecture DynFire to provide dynamic firewalling. It can perform attribute-based access control to decide which user can access firewall secured resources. DynFire as such cannot be a solution for the whole Internet. Instead, it can be used to secure the IT resources of a single organization. It is assumed that this organization operates a network that is protected from the Internet by firewalls. The DynFire administrators do not create firewall rules based on individual IP addresses, but describe the desired communication relationship between users and services (network resources) in an administration panel in the form of policies.

Figure 1 shows the concept of DynFire. When a user logs into the network he receives a temporary IP address. The "Firewall Manager" uses the temporary binding between user and IP address and the policies to create firewall rules, which are related to a single device used by a single user. Those firewall rules are valid as long as this particular user is logged in. In a complex network topology the Firewall Manager has to configure all firewalls on the paths between the users and the resources, respectively. The architecture is shown Figure 2 and each main component is introduced in this section.

A. Policy Config GUI

The Policy Config GUI is the central instance to administrate all policies of the system. Every administrator and owner is able to login and control its assigned zones. Additional administrators have the possibility to enter policies for their users in very comfortable way as already described.

B. Network Access Device

The network access device is responsible for authenticating and logout of the user. It creates context information about the user e.g., from which location the user is logged in. This context information will be carried along the username and the IP address to the policy controller.

C. Policy Controller

When the Firewall Manager is notified about the login and temporary binding between UserID and IP address is received. It executes an access evaluation algorithm with will be described later in this paper. The algorithm returns a set of permissions, which permits the user to access all for him enabled services. These permissions contain the IP address of the resource, the port of the service, and the transport layer protocol (TCP or UDP) used by the service. The source IP address was passed by the network access device. Firewall 5-tupel rules can be generated from these data. In specific cases where protocols using dynamic ports are involved, additional information about the service is sent together with it. These additional information advices the firewalls to deploy this firewall rule in a special manner. For example, the firewall has to activate a connection tracking module to be aware of related connections. These related connections have to be accepted as well. Information about the concerned firewalls is retrieved from the Topology Awareness Module. Then, the rules are sent to the Firewall Provisioning Module. In case of a logout the Policy Controller remove all associated rules for the user.

D. Topology Awareness Module

The Topology Awareness Module has to find all firewalls on the path between two given hosts. Therefore, it has to know the network topology. The current version is able to work with a static topology map. An advanced version that can detect the topology automatically based on LLDP (Link Layer Discovery Protocol) [4] and SNMP (Simple Network Management Protocol) [5], is currently under development. It will also interact with the routing protocol, in order to configure firewalls on the alternative path, in case a rerouting occurs.

E. Firewall Provisioning Module

The Firewall Provisioning Module is responsible for transferring firewall rules to a set of firewalls. Several protocols for firewall control exist [6]. The SIMCO protocol [7] was chosen, because of its flexibility and simplicity. Several SIMCO implementations for Linux (iptables), Cisco, and Juniper routers are currently under development or testing. Furthermore it is possible to integrate the Firewall Manager into the Astaro Command Center [8], which provides an integrated firewall solution. This multitude of supported firewalls allows DynFire to be deployed in heterogeneous network environments.

 ISBN: 978-1-61208-231-8

III. Policy Framework

Common access models like RBAC [9] or ABAC [10] (which is used in this work) are very abstract specified models and not suitable for an implementation. They do not deal with the problem "HOW" a rule can be evaluated. If one does not find a suitable representation of your rules, the model still works but it will become nearly impossible to administrate, because rules could become to complex to define by network administrators. However, ABAC is a generic model that describes neither how the attributes and the evaluation function look like, nor how the evaluation process works. We developed a representation of high-level policies, which provide an intuitive way to grant access to firewall secured resources and an efficient way to evaluate firewall rules.

A. Capabilities

In the following, each main feature is described in detail and why it is needed.

1) Policy Definitions: In DynFire, a policy describes how a user can access a resource or a server. In particular:

> Under which **condition** a **user** can access a **service** on a **resource**.

A typical example would be a policy like:

> "Bob can access the wiki of his institution during daytime."

DynFire adds additional possibilities for a fine granular definition of conditions. So, it could also be possible to define a policy like:

> "Alice can access the ssh-server only if the intrusion detection system of the network set its client health value 5 or more and she is connected via VPN, but not via WiFi."

The Policy Framework refers to three different terms here. The **Who** is already determined during the login process. The **condition** is a logic that grants access if all associated credentials match.

Services: DynFire associates services with subsets of a host. In common firewall understanding, a service is described by its port. Typically, this is also true for DynFire; but, in addition, there can be more information to describe abstract services like âIP-telephonyâ.

Not all firewalls may support all different type of services. So the interpretation of the service description has to be done at the provisioning level of the DynFire firewalls.

Resources: A resource is typically a host or a group of hosts where a service is running on. The hosts themselves are identified by their IP addresses. This means that resources are typically a set or range of IP addresses.

2) Multitenancy Capabilities and Delegation: As described in the introduction of this paper, DynFire is targeted at medium to large scale networks. In particular, this means the administrative tasks like granting access to a resource can not be done by a single administrator, especially if the corresponding Resources are not within his administrative domain. Following the structure of big organizations, DynFire divides the network into different parts based on their networks and subnets.

This means that the top administrator owns all network resources and may split them into different parts. Each part is represented as a subset of the original network. Those subsets can be assigned to other administrators that can assign policies for their subset of the network but not for other subsets. This allows DynFire to provide a scalable administrative hierarchy that decentralizes the responsibilities in the network.

3) User Groups: To handle a potential big number of users, DynFire administrators can group users. Besides normal assignments of access control to users, the same should be possible for groups. Groups may defined by any administrator in their administrative domain. It is also possible to add groups to other groups and create recursive group definitions for better usability and scalability of the group definitions.

4) Context-sensitive Rule Evaluation: Since mobility has has grown importance, this is reflected by adding context-sensitive functionality to the framework. A user may access the network via different networks and devices. This can be reflected in the defined rules, like allowing unencrypted mail access only over a secured connection.

5) Audibility: In distributed administrated network it should always be possible to track the changes and know who is responsible for the changes. In DynFire, it is possible to restore any state of the Policy Framework in the past a check who changed the configuration. This is mostly motivated by legal requirements and in order to allow analysis during or after attacks on resources in the network.

B. Components

The Policy Framework implements some basic components required for the policy specification and rule evaluation. It is capable to extend this list by any parameters users provide during the login process.

DynFire uses some terminology that will be described in this section. Most of the terms are much overloaded in the literature. We tried to align the common understanding of those terms with the functionality of DynFire. Figure 3 shows a possible implementation of the frameworks. The different entities will be described in this section.

1) Credential: ABAC is based on attributes. In this case, the attributes are represented by credentials. Credentials can be assigned to users by administrators or they are formed during the login process of users. Also, every permission,

 ISBN: 978-1-61208-231-8

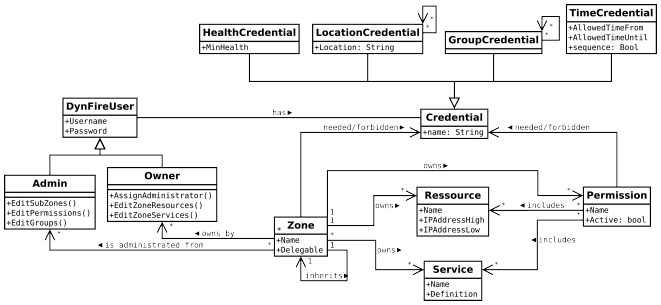


Figure 3. DynFire Policy Model

which is required for getting access on a service running on a corresponding resource, has a list of credentials users need to have for getting access. In addition, there is a list including forbidden credentials. Thus, if a user possesses a credential which is element of=20 such a list, it is not possible for one to get such a permission. Each credential technically is evaluated in the same way. This means that there can be additional credentials added over time, especially without adding additional source code in the policy evaluator. The design itself allows adding additional parameters that must (or must not) match the user credentials.

The implementation of DynFire currently considers four kinds of Credentials:

(a) Group credentials
A group only allows access to a resource if the user is in the required group. As shown in Figure 3, a group can contain itself. This results in the possibility to implement recursive groups. The side-effects, like looped groups, are resolved in the database through stored procedures which is the common solution to keep data consistency.

(b) Location credentials
A location credible typical is set in the login process. This information is typically passed from the login program. For example, if the user logs in via VPN, the VPN login process can set the parameter. Based on this information the user may be granted access to the resources or not. Other possible location credentials are 802.1X [11] (e.g., WiFi) or any other network authentication method to map an IP address to a user.

(c) Health credentials
An external entity provides information about the host that the user uses to login. During the policy evaluation process, this value is checked against the specification in the policy and have to match the minimum value. For example, a intrusion detection system can scan the host for possible security holes or the Network MAC address is known by the anti-virus software of the network and provide the information that the logged in system runs the newest virus scanner.
It can be a simple value like “secure” and “not secure”. It can also provided a fine granular specification like a range from 1-100, 10 for example, would means a low security status.

(d) Time credentials
A time credential enables the specific permission only during a fixed time. Typically, this can be used to allow access to a resource only during the working days.

2) Permission: A permission in the Policy Framework is a combination of:

(a) required credentials
(b) forbidden credentials
(c) resources
(d) services

This means that the users, which possess all needed credentials (a), and none of the forbidden ones (b), have access to the resource (c) via the service (d). A simple example is that the user Bob from VPN can access the server 192.168.123.15 via ssh if he is belonging to group Administrators and did not login via WiFi.

3) Zones: To separate different subnets from each other the term “zone” is introduced. A zone is collection of network or IP ranges. The root zone contains the complete network managed by the Policy Framework. This network can have some child that contains a subset of the network(s) of this root zone. Let

$$M_f = \{net_{f1}, net_{f2}, net_{f3}, ...\} \quad (1)$$

be zone where net_x is a network in CIDR notation with the relation $\subseteq$. A network $n_i \subseteq n_j$, when all IP addresses of the network n_i are in the network n_j. Let

$$M_c := \{net_{c1}, net_{c2}, net_{c3}, ...\} \quad (2)$$

be child zone of M_f. Then following is true:

$$\forall net_{cx} \in M_c, \exists net_{fn} \in M_f : net_{cx} \subseteq net_{fn} \quad (3)$$

This means that each network in a sub-zone has to be in one of the networks in the parent-zone. This also implies that a network may be member of multiple sub-zones. Figure 4 shows a simple example of a zone structure. Each zone has its own required and forbidden credentials to define what credentials are needed to access the resources of this zone.

Admins and Owners: Administrators and owners are two central administrative entities in the Policy Framework. Each zone has a least one administrator and one owner. Both have different roles in the framework. An owner is - as it says - the owner of the sub-zone. This typically, does not mean that this user administrates the zone. He has the ability to assign administrators to his zone and split the zone in different sub-zone for further delegation.

 ISBN: 978-1-61208-231-8

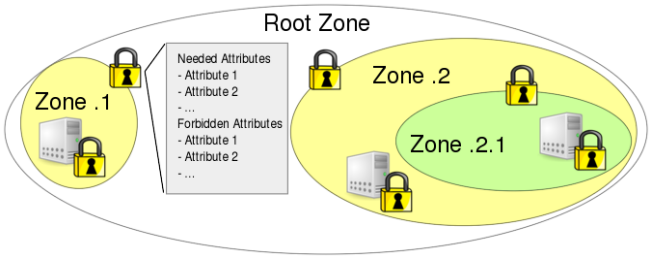


Figure 4. DynFire zone structure example

An administrator defines local groups, services, resources and finally permissions to a zone. Of course, an owner of a zone can assign the administration tasks to his own account.

C. Access Evaluation Algorithm

In contrast to other access control systems, users access rights are not checked in the event of an access attempt. Instead after a successful authentication of the user, all necessary firewall rules should be deployed on all related firewalls in the network at once. As already mentioned, permission is the aggregation of a service, a resource, and all required and forbidden credentials. Therefore an efficient algorithm to find out all enabled permissions for a user, is needed. Let Z the set of all zones exiting in the Policy Framework. Let C_{ZN} the list of credentials, which are needed to access a zone. For Zone z, that would be C_{ZNz}. Let C_{ZFz} the list of forbidden credentials. C_{PNz} and C_{PFz} are of the same kind but are belonging to permissions. Let C_U the set of credentials the user owns. Let Z_A the set, which includes all zones the user is allowed to access. It is defined as follows:

$$Z_A = \{z \in Z | ((C_{ZNz} \subseteq C_U) \wedge (C_U \bigcap C_{ZFz} = \emptyset))\} \quad (4)$$

The user is allowed to access a zone if the needed credentials to access the zone are a subset of the attributes of the user. Also the user must not have a credential which is forbidden. Due to the nature of inheritance of the zones, follows that no one can access resources from a zone, which inherits from a zone on which the user is not allowed to access. Thus, not all zones have to be searched. Because if a zone that the user is not allowed to access is found traversing a branch, you can break up and go on with the next branch. After figuring out the zones, which the user is allowed to access, all permissions inside these zones, enabled for the user, have to be evaluated. So one have to check all permissions, if the user has all needed credentials, which are necessary for permission. In addition the user must not have an attribute, which is forbidden for this permission. This results in:

$$P_A = \forall_{z \in Z_A} \{p \in z | ((C_{PNz} \subseteq C_U) \wedge (C_U \bigcap C_{PFz} = \emptyset))\} \quad (5)$$

The result is a set permission which can be converted into firewall rules. Since this contains only rules that allow connections and not forbid them, the order of the rules is irrelevant. So, there can not be any conflicts between those rules.

IV. Related Work

Dynamic control of firewalls has been studied in detail for Voice over IP applications [12], [6], [13]. Cisco Systems's TrustSec technology [14] can deploy "downloadable Access Control Lists" (dACL) when a user connects to the network. However, this is currently a vendor-specific solution.

Bartal et al. [15] present a firewall management toolkit with includes a management language for abstract firewall rules, but every change of the rule set result in a recompilation of the whole model code. Due to the distributed structure, this could become a bottleneck in DynFire.

Frèdèric Cuppens et al. [16] proposed a framework for describing rules for different firewalls, but the solution is more focused on the description of a firewall rule. This framework also does not regard the group or user based access control. Instead, they grant access on a per host basis.

Laborde et al. [17] used a general RBAC model to design a Policy-based network management (PBNM) system, but kept open if it is possible to implement it into a real network due to its complexity.

Basile et al. [18] designed and evaluated an ontology-based security policy system for networks. They regard the administrative task but also do not regard the dynamic login of different users. They also assumed that a user uses a fixed workstation and so the user could not change the location.

Zhang et al. [19] defined a high-level specification language. Their approach detects conflicts in the rule specification but can not automatically deal with it. The Policy Framework we propose does not allow the specification of deny rules and completely avoid any conflicts in the rule generation.

XACML [20] is a very detailed policy description language and was investigated during the specification phase. The specifications of XACML is not powerful enough to fit the requirements, e.g., describing the distributed administration. An overview about the complete DynFire architecture is given in [21]. This also covers the other developed modules.

V. Conclusion and Future Work

ABAC provides a solid basis for implementing an attribute-based policy framework. Nevertheless, a realization of such a framework imposes high complexity in the evaluation of the policies and the administration. This paper

 ISBN: 978-1-61208-231-8

presented the Policy Framework of DynFire, an ABAC-based framework for the dynamic modeling and deploying of firewalls. It enables attribute-based access to network resources.

We currently deploy DynFire in the campus network of the University of Stuttgart. While finishing the implementation, we are also evaluating and analyzing the performance, scalability, and security of DynFire.

ACKNOWLEDGMENT

This work was supported by the "DynFire" project [22], a research project supported by the German Federal Ministry of Education and Research (BMBF, Foerderkennzeichen: 01BY1151). The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the DynFire project or the BMBF.

The authors would like to thank Christoph Schock and Dominik Lamp for contributions and feedback.

REFERENCES

[1] R. Oppliger, "Internet security: firewalls and beyond," *Commun. ACM*, vol. 40, no. 5, pp. 92–102, May 1997.

[2] S. M. Bellovin and W. R. Cheswick, "Network firewalls," *IEEE Communications Magazine*, vol. 32, pp. 50–57, 1994.

[3] D. B. Chapman and E. D. Zwicky, *Building Internet Firewalls*, 1st ed., D. Russell, Ed. Sebastopol, CA, USA: O'Reilly & Associates, Inc., 1995.

[4] IEEE LAN/MAN Standards Committee, "Station and Media Access Control Connectivity Discovery," IEEE, Std. 802.1ab, 2009.

[5] J. Schoenwaelder and T. Jeffree, "Simple Network Management Protocol (SNMP) over IEEE 802 Networks," IETF, RFC 4789, Nov. 2006.

[6] S. Kiesel and M. Scharf, "Modeling and performance evaluation of transport protocols for firewall control," *Computer Networks*, vol. 51, no. 11, pp. 3232–3251, Aug. 2007.

[7] M. Stiemerling, J. Quittek, and C. Cadar, "NEC's Simple Middlebox Configuration (SIMCO) Protocol V3.0," IETF, RFC 4540, May 2006.

[8] "Astaro, a Sophos Company," http://www.astaro.com, [retrieved: Oct., 2012].

[9] D. F. Ferraiolo and D. R. Kuhn, "Role-based access controls," *15th National Computer Security Conference*, pp. 554–563, 1992.

[10] J. M. Torsten Priebe, Eduardo Fernandez and GÃ$\frac{1}{4}$ntherPernul, "A pattern system for access control," in *Research Directions in Data and Applications Security XVIII*, ser. IFIP International Federation for Information Processing, C. Farkas and P. Samarati, Eds. Springer Boston, 2004, vol. 144, pp. 235–249.

[11] IEEE LAN/MAN Standards Committee, "Port-Based Network Access Control," IEEE, Std. 802.1x, 2004.

[12] C. Aoun, "Plan de signalisation Internet pour l'interfonctionnement entre NAT et Firewall," PhD Thesis, ENST, Paris, 2005.

[13] ETSI TISPAN, "NGN Functional Architecture," ETSI, Standard ES 282 001 V3.4.1, 2009.

[14] Cisco Systems, Inc, "Cisco TrustSec Solution Overview," http://www.cisco.com/en/US/netsol/ns1051/index.html, [retrieved: Oct., 2012].

[15] Y. Bartal, A. Mayer, K. Nissim, and A. Wool, "Firmato: A novel firewall management toolkit," *ACM Trans. Comput. Syst.*, vol. 22, no. 4, pp. 381–420, Nov. 2004.

[16] T. S. Frèdèric Cuppens, Nora Cuppens-Boulahia and A. Miège, "A formal approach to specify and deploy a network security policy," in *Formal Aspects in Security and Trust'04*, 2004, pp. 203–218.

[17] F. B. Romain Laborde, Michel Kamel and A. Benzekri, "Implementation of a formal security policy refinement process in wbem architecture," *J. Netw. Syst. Manage.*, vol. 15, no. 2, pp. 241–266, Jun. 2007.

[18] C. Basile, A. Lioy, S. Scozzi, and M. Vallini, "Ontology-based policy translation," in *Computational Intelligence in Security for Information Systems*, ser. Advances in Intelligent and Soft Computing, A. Herrero, P. Gastaldo, R. Zunino, and E. Corchado, Eds. Springer Berlin / Heidelberg, 2009, vol. 63, pp. 117–126.

[19] B. Zhang, J. R. Ehab Al-Shaer, Radha Jagadeesan, and C. Pitcher, "Specifications of a high-level conflict-free firewall policy language for multi-domain networks," in *Proceedings of the 12th ACM symposium on Access control models and technologies*, ser. SACMAT '07. New York, NY, USA: ACM, 2007, pp. 185–194.

[20] "Xacml spezification - oasis extensible access control mark-up language," http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml, [retrieved: Oct., 2012].

[21] A. Vensmer and S. Kiesel, "Dynfire: Dynamic firewalling in heterogeneous environments," in *Internet Security (WorldCIS), 2012 World Congress on*, June 2012, pp. 57 –58.

[22] "DynFire project home page," http://www.dynfire.org, [retrieved: Oct., 2012].

 ISBN: 978-1-61208-231-8

Formal Characterization and Automatic Detection of Security Policies Conflicts

Hédi Hamdi
Manouba University, ESC
Campus Universitaire de la Manouba
2010 Manouba, Tunisia
Email: hamdi.h@gmail.com

***Abstract*—Policies, which are widely deployed in networking services (e.g., management, QoS, mobility, etc.), are being a promising solution for securing wide distributed systems and one of the most actual directions of research in the information security area. However, Policy-based security may involve interactions between independent decision making components which may lead naturally to inconsistencies, a problem that has been recognized and termed as policy conflict. Work on policy analysis has mainly focused on conflicts that can be determined statically at compile time. Using formal methods, with good tool support, to express the policies, can not only support the detection, but also help all the involved actors in understanding and resolving the conflicts. The main focus of this paper is on giving a theory and automated techniques for discovering common types of security policy conflicts.**

Keywords-Policies; Distributed systems; Conflicts; Detection.

I. INTRODUCTION

Policies, which are extensively deployed in networking services (e.g., management, QoS, mobility, etc.), are being praised as promising solution for securing widely distributed systems and could also be considered as one of the most recent directions of research in the information security field. However, several problems remain to be solved in this field. One interesting problem of policy based security is how to detect conflicts in a security policy specified for a network behavior. In fact, deploying a conflicting policy within a network is often the origin of unexpected damage. For this reason and once policies are specified and before they are enforced, it should be possible to determine that there are no conflicts between components of the policy. Previous works on issue of policy conflict detection have mainly focused on conflicts that can be determined statically at compile-time [12]. The detection process involved simple policy analysis. Although we believe that static analysis is very useful for detecting some conflicts before policies are deployed, it cannot detect many conflicts in resource management policies which occur as a result of the current state of the resources. For example, policies which increment or decrement allocation of resources may conflict with policies related to setting upper and lower bounds for the resources. These conflicts result from current state of the resource allocation and bounds so can only be detected at run-time. This paper focuses on the PPL (Policy Programming Language) [5][6] a domain specific policy language with a powerful dynamic semantic and with available Software tools, based on which techniques for aiding policy analysis and refinement can be developed.

The work presented in this paper addresses the shortcomings in previous work in the field. It defines a formal model to deal with a range of conflicts in security policy, and an algorithmic solution to facilitate automation of the analysis process.

This paper begins by stating the problem of conflict detection in Section 2, followed by a presentation of our policy model in Section 3. Section 4 introduces a formal model for conflicts detection in security policy. Section 5 presents an algorithmic solutions to the automation of the analysis process and Section 5 concludes the paper and discusses future Works.

II. PROBLEM STATEMENT

In recent years, the trend in the software industry has been directed towards the development of software that can be customized by the user to meet their individual needs. In this context, policies are a very useful way in which the customization can be delivered. Policies also separate the behavioral aspect of software and its main functions. This allows either the main functionality of the software or custom user's behavior to be changed without affecting the other [12]. In a given system, there may coexist multiple policies, it is important to consider how one policy will affect another. Policies that are triggered at the same time, and they contradict each other, are said in conflict. The process of checking policies to see if they conflict is called policy analysis, and conflicts can be detected at specification time. By Lupu and Sloman [12], two types of conflicts can occur between policies: modality conflicts and semantic conflicts (also called application specific). In their work, they associated policies with a mode. According to their definition, a modality conflict arises when two policies with opposite modality refer to the same subject, actions, and objects. This can happen in three ways:

- The subjects are both obligated-to and obligated-not to perform actions on the objects.
- The subjects are both authorized and forbidden to perform actions on the objects.
- The subjects are obligated but forbidden to perform actions on the objects.

 ISBN: 978-1-61208-231-8

Application specific conflicts occur when two rules contradict each other due to the context of the application. We use for our policy model, the PPL (Policy Programing Language) [5][6], our policy specification language (PSL) that appears to be the most flexible. It offers both positive and negative modifications of authorization and obligation policies. Although we do not focus on policy entry in this paper, we assume that all policies entered into the system are done so in the form of PPL language.

III. OUR POLICY MODEL

A. PPL: The Policy Programming Language

We use a domain-specific, special-purpose language to express security policies. The design of our language has been guided by a thorough study of the domain of computer security in general, and especially security based policies. We examined various kinds of tools mainly including specifications of known security policies, specification for typical security policy (e.g., IPSec policy [13]) as well as more dedicated ones (e.g., web services security Policy [10], Security Policy for web semantic [8] and Security Policy for Clinical Information Systems [1]), frameworks and tools for security policy specification (e.g., Ponder [3], PDL [11]), and various documentations and articles. Based on this domain analysis, we have identified the following key requirements for a language dedicated to this domain. The language should be composed of five basic blocks: entities, scopes, rules, actions and policies to describe the appropriate operation performed for ensuring security of a given system; it should include block-specific declarations to enable dedicated verifications and analysis to be performed; it should be modular to enable a security policy specification to be decomposed into manageable components and also policies can also be composed into more complex policies until it forms a global and single policy; it should include an interface language to enable disciplined re-use of existing security actions libraries.

B. Core Concepts of PPL

A PPL program essentially defines a list of blocks. Blocks declarations describe which subjects (e.g., users or processes) may access which objects (e.g., files or peripheral devices) and under which circumstances. A block can either be a policy, a rule, an action or an entity, a scope. Scope represents a list of entities involved in policy. Policies correspond to a sequence rules to determine specific configuration settings for some protection of system; they can be either simple or compound. A simple policy refers to a list of protection action implemented in some other programming language. This facility enables existing actions libraries to be re-used. A compound policy is defined as a composition of simple policies. Rule consists of a set of constraints on a set of actions; they can be either a single-trigger where only one action is triggered for a given object or a multi-trigger where multiple different actions may be triggered for the same object. Action can be atomic or compound in the following we present in details each of the basic blocks comprising PPL and show how they are used in writing PPL security policies.

```
PPLSpec    ::= blocks
Blocks     ::= block j block blocks
Block      ::= rule | policy| action| scope| entity
```

Fig. 1. Syntax of a PPL specification

1) Entities

PPL entities are typed objects with an explicit interface by which their properties can be queried. Entities can be an object or a subject or a collection of them. They have identification and can be a source and a destination of rules.

2) Scopes

Entities can be collected into Scopes. Scopes are essential in any policy considering that they provide the necessary abstraction to achieve compactness, generalization and scalability. Without Scopes, each rule has to be repeated for each entity to which the rule applies. Scopes have a name and they are used in rules for simplified management of large numbers of entities. PPL offers two types of scopes: classes and domains. Classes are sets of entities that are classified according to their properties e.g., all TCP packets, and domains are sets defined by explicit insertion and removal of their elements.

3) Policies

A PPL policy is a group of rules and scopes that govern particular domain events. These rules are used to define the right behavior of a system. PPL supports an extensible range of policy types:

- Authorization policies are essentially security policies related to access-control and they specify whether a sequence of actions, a subject, is permitted or forbidden to perform to a set of target objects. They are designed to protect target objects, so they are interpreted by access control system.

```
policy ::= type-pol policy ident ((params))?{
           policy-def }
type-pol ::= pauto | nauto policy-def ::= scope-def
           body-def (constraint-def )?
scope-def ::= scope: { scope}
body-def ::= body: rules
rules     ::= rule;| rule; rules
constraint-def ::= while: expr
```

- Obligation policies specify what a sequence of actions, a subject must perform to a set of target objects, on response to particular events and define the duties of subjects in scope of policy. Obligation policies are normally triggered by events.

 ISBN: 978-1-61208-231-8

```
policy              ::=  type-pol policy ident ((params))?
                         {policy-oblig-def}
type-pol            ::=  poblig | noblig
policy-oblig-def ::= event-def scope-oblig-def
                         body-oblig-def (constraint-def )?
scope-deleg-def ::= subject: { scope}
                         (object: { scope})?
body-deleg-def  ::= body:actions
event-def           ::= event:expr
actions             ::= action;| action;actions
constraint-deleg-def ::= while: expr
```

- Delegation policies specify which actions and rights subjects can delegate to others. A delegation policy thus specifies an authorization to delegate.

```
policy     ::=      type-pol policy ident
                    ((params))?{deleg-def}
type-pol   ::=      pdeleg j ndeleg
deleg-def  ::=      scope-delegbody-deleg
                    (constraint-def )?
scope-deleg ::=     (subject: { scope})?(object: { scope})?
                    (recipient: { scope})?
body-deleg ::=      body:(associated-authorization)?actions
associated-authorization ::= auto-policy:indent
actions    ::= action;| action;actions
constraint-deleg-def ::= (while: expr)? (cnumber:type-int)?
```

- Compound policies are used to group a set of related policy specifications within a syntactic scope with shared declarations in order to simplify the policy specification task for large distributed systems.

4) Rules

A rule consists of a set action that subjects can perform on target objects when a set of constraints are satisfied. In single-trigger rule, only one action is triggered when condition is satisfied. In a multi-trigger, multiple different actions may be triggered for the same object when condition is satisfied. For example, IPSec crypto-access rule is a single-trigger. In fact, once traffic matches a certain condition, its action is triggered and no further matching is performed. This is in contrast to crypto-map rules where a particular traffic may match multiple constraints causing multiple actions to be triggered.

```
Rule                ::=  rule ident ((params))? { rule-def }
rule-def            ::= {subjects-def subjects-def  constraints-def}
subjects-def  ::= subject:entities
objects-def   ::= object:entities
constraints-def ::= constraint | constraint constraints-def
constraint          ::=  if (expr ) then actions
actions             ::= action;| action; actions
```

5) Actions

Actions represent the operations triggered when a constraint match. Actions can be either atomic for example in IPSec filtering policy, actions are protect, bypass, discard, or composite such as a service implementation.

IV. FORMAL MODEL OF CONFLICTS DETECTION

There are two broad categories of policy conflicts namely static and dynamic conflicts. As conflict detection can be computationally intensive, time consuming and therefore costly and would preferably be done statically, at compile time. Identified static conflicts therefore require immediate attention, as it will most certainly result in a conflict at some time. Whereas the transformation of a potential, dynamic conflict in a real conflict is quite unpredictable; that is, the inconsistency may be exposed temporarily, or indeed not all. The main purpose of conflict detection is:

- The identification of actual conflict that has occurred and can be resolved statically, at compile-time.
- The prediction of a conflict, that may, occur in the future (and more specifically, exactly what circumstances will expose that conflict)

It should be noted, however, that all the predicted conflicts require notification or action. In some cases, for example, conflict can be predicted to occur, but be far enough into the future or uncertain enough that an alert has no real importance and action would be inappropriate at present. To be able to detect conflicts statically and at runtime, one must know the temporal characteristics of policies in the specification. To do that, we define $start_{t/e}(P)$ that refers to time/event start attribute of the policy, $finish_{t/e}(P)$ that refers to time/event finish attribute of the policy, $recurt_{t/e}(P)$ that refers to time/event recur attribute of the policy and *constraint(P)* which returns the constraint of the policy.

A. Static conflicts detection

1) Authorization conflicts

a) Conflict between two policy rules

□ $(Subject(R_x) \cap Subject(R_y) \neq \phi) \wedge (Object(R_x) \cap Object(R_y) \neq \phi) \wedge (Action(R_x) = DENY) \wedge (Action(R_y) = PERMIT) \rightarrow authoConflict(R_x;R_y)$

Conflicts in a set of policy rules

Let R a set of security rules, $|R|$ the cardinality of R

□ $0 \leq i \leq |R|;\ \forall 0 \leq j \leq |R|$
$\exists R_i;\ R_j \in R \wedge authoConflict(R_i;R_j) \rightarrow RConflict(R)$

b) Conflicts between two policies

We denote a PPL policy by *P(S; B; C),* where S designates the scope of *P* policy, *B* indicates its Body and *C* the policy constraint. The detection of authorization conflicts process within the same policy, can generalized to detect conflicts in a set of authorization policies. However, it is necessary to

ensure that these policies have equivalent constraints (if it is defined, the specification of the constraint in an authorization policy is optional in PPL), they must run in the same period.
Let $P_1 (S_1, B_1, C_1)$, $P_2(S_2, B_2, C_2)$ two authorization policies. P_1 and P_2 are in conflict:

- $(start_t(P_2) < finish_t(P_1)) \wedge (start_t(P_1) < finish_t(P_2)) \wedge (constraint(P_1) \equiv constraint(P2)) \wedge RConflict(B_1 \cap B_2) \rightarrow PConflict(P_1,P_2)$

2) Obligation conflicts

- $\forall start_t(P_2); finish_t(P_2); recurt(P_1); start_t(P_2) < recur_t(P_1) < finish_t(P_2) \rightarrow PConflict(P_1;P_2)$

- $\forall start_t(P_2); recur_t(P_1); finish_e(P_2) (start_t(P_2) < recur_t(P_1) < finishe(P_2)) \rightarrow PConflict(P_1;P_2)$

B. Dynamic conflicts detection

- $\forall finish_t(P_2); Recur_t(P_1); start_e(P_2) (start_e(P_2) < recur_t(P_1) < finish_t(P_2)) \wedge (trigger(start_e(P_2))) \rightarrow PConflict(P_1;P_2)$

- $\forall recur_t(P_1); start_e(P_2); finish_e(P_2) (start_e(P_2) < recur_t(P_1) < finish_e(P_2)) \wedge (trigger(start_e(P_2))) \rightarrow PConflict(P_1;P_2)$

- $\forall start_t(P_2); finish_t(P_2); recur_e(P_1) (start_t(P_2) < Recur_e(P_1) < finish_t(P_2)) \wedge (trigger(start_t(P_2))) \rightarrow PConflict(P_1;P_2)$

- $\forall start_t(P_2); finish_e(P_2); Recur_e(P_1) (start_t(P_2) < recur_e(P_1) < finish_e(P_2)) \wedge (trigger(start_t(P_2))) \rightarrow PConflict(P_1;P_2)$

- $\forall finish_t(P_2); start_e(P_2); Recur_e(P_1) (start_e(P_2) < recur_e(P_1) < finish_t(P_2)) \wedge (trigger(start_e(P_2))) \rightarrow PConflict(P_1;P_2)$

- $\forall start_e(P_2); finish_e(P_2); recur_e(P_1) : event_j start_e(P_2) < Recur_e(P_1) < finish_e(P_2) \wedge (trigger(start_e(P_2))) \rightarrow PConflict(P_1;P_2)$

V. AUTOMATING THE POLICY ANALYSIS

A. Modality conflicts detection

The precondition for a modality conflict occurs is that policy containing rules using the same subjects, similar actions, the same objects, and the same constraints, take effect at the same period. Therefore, it is necessary to know the time on which a policy will be enforced (for checking inter-policy), and so brought their overlap. The intra-verification of policy seems simple enough. Indeed, the analysis of a policy specification, allows enumerating all tuples (subject, object, action) on which policy rules are applied. If two or more rules that are applied to a single tuple (subject, object, action), then there is a potential conflict and policy must be checked to see if there is a real conflict (e.g., a rule authorization and a prohibition rule applied to the same tuple (subject, object, action)). A modality conflict can be one of the following types:

1) Authorization Conflict

A modality conflict of authorization occurs when a positive authorization rule and a negative authorization rule are defined for the same subjects, objects. The following algorithm is used to detect authorization conflicts between two rules.

Algorithm 1: two rules Conflict

```
authConflict_R(R1;R2) : Boolean
begin
        s1 := GetSubject(R1),s1 := GetSubject (R2)
        o1 := GetObject(R1),o1 := GetObject (R2)
        a1 := GetActiont(R1), a1 := GetAction (R2)
        if ((s1 = s2) and (o1=o2) and (a1 = DENY) and
        (a2 = PERMIT)) then
                TRUE
                else
                FALSE
end
```

The procedure for detecting conflicts between rules is used in a generic procedure which determines all the rules in conflicts in the specification of a policy. It returns an array containing a structure of rules in conflict. Below, we present this procedure.

Algorithm 2: Conflict in set of rules

```
begin
        RS:structure
        begin
                R1 : rule
                R2 : rule
        end
        Tab_RS: array of structure RS
        Tab_R: array of rules
        Tab_P: array of policies
        authConflict_P (P): Tab_RS
        tab1 : tabR
        tab2 : tabRS
        i, j, k, l: integer
        K =1
        tab1 ← get_R (P)
```

```
        for (i = 1; i < (tab1.lenght) - 1; i + +) do
        for (j = i + 1; j < (tab1.lenght); j + +) do
                if(authConflict_R(tab1[i];tab1[j])=
                TRUE) then
                tab2[k]:R1 = tab1[i]
                tab2[k]:R2 = tab1[j]
                K + +;
end
```

The authorization conflicts detection process within the same policy can be generalized to detect conflicts between different authorization policies. However, the prerequisite for the occurrence of a modality conflict is that the policies involved hold at the same time. Besides, it is essential to take into account the constraints that control the applicability of the policy. This greatly complicates the conflict detection procedure. To overcome this problem, we define the *commence(P)* function, which returns the time from which the execution of *P* policy begins, the *finish(P)* function, that returns the time of P policy execution ends, and the *constraint(P)* which returns the *P* policy constraint. Below we present the two policies conflicts detection procedure.

Algorithm 3: two policies conflicts

```
authConflict_interP (P1; P2; tab3; k)
begin
        tab1; tab2 : tabR;
        j, i : integer;
        var c: Boolean
        K =1;
        tab1 ← rename(get_R (P1));
        tab2 ← rename (get_R (P2));
        if ((commence(P2) < finish(P1)) and ( finish(P2)
        > commence(P1)) and (constraint(P1)
        =constraint(P2))) then
                for (i = 1; i < (tab1.lenght); i + +) do
                        for (j = i+1; j < (tab1.lenght); j
                        ++) do
                        if (authConflict_R ( tab1[i];
                        tab2[j]) = true) then
                        tab3[k]:R1 = tab1[i];
                        tab3[k]:R2 = tab2[j] ;
                        K + +;
                        C= TRUE;
                        else
                        C= FALSE;
end
```

The generalization of this procedure can detect conflicts between different authorization policies.

Algorithm 4: set of policies conflicts

```
authConflict_interP(tab: Tab_P);
begin
        tab1 : tabRS;
        k: integer;
        K =1;
        for (i = 1; i < ((tab.lenght) - 1); i + +) do
                for (j = i + 1; j < (tab.lenght); j + +) do
                authConflict_interP (tab[i]; tab[j]; tab1; k);
end
```

2) Obligation conflicts

This type of conflicts occurs if one policy specifies that a subject is obliged to perform an action when another policy requires that the subject refrain from performing that action. This type of conflict is determined by the following procedure

Algorithm 5: Obligation conflict

```
obligConflict(P1; P2): boolean
begin
        t1 ← getType_P(P1);
        t2 ← getType_P (P2);
        S1 ← getSubjet_P (P1);
        S2 ← getSubjet_P (P2);
        O1 ← getObjet_P (P1);
        O2 ← getObjet_P (P2);
        A1 ← getAction_P (P1);
        A2 ← getAction_P (P2);
        if ((commence(P2) < finish(P1)) and
        (finish(P2)>commence(P1)) and (constraint(P1)
        =constraint(P2)) and (t1 = POBLIG) and (t2 =
        NOBLIG) and (S1 =S2) and (O1 = O2) and
        (A1 = A2)) then
                TRUE
                else
                FALSE
end
```

a) Unauthorized Obligation Conflicts

This type of conflict occurs if a subject is obliged to perform an operation; but, there is another policy that prohibits the subject from performing the operation.

Algorithm 6: Unauthorized Obligation Conflicts Detection

```
unauthObligConflict(P1, P2): Boolean
begin
        tab: tab_R;
        i: integer;
        t1 ← getType_P(P1);
        t2 ← getType_P (P2);
        S1 ← getSubjet_P (P1);
        O1 ← getObjet_P (P1);
        Tab ← get_R(P2);
```

if ((commence(P_2) < finish(P_1)) and (finish(P_2) > commence(P_1)) and (constraint(P_1) =constraint(P_2)) and (t_1 = POBLIG) and (t_2 = NAUTO)) **then**
for (i = 1; i < (Tab:lenght); i + +) **do**
if (((GetSubject(Tab[i]) = S_1), (GetObject(Tab[i]) = O_1) and GetActiont(Tab[i]) = DENY)) **then**
TRUE
else
FALSE
end

VI. Related Work

Research in conflict analysis has been actively growing over the years, but most of the work in this area addresses general management policies. The authors in [12] focused on identifying modality conflicts by simple analysis between positive and negative authorization security policies and the specification of policy precedence rules in order to resolve conflicts. Jajodia [7] has proposed a technique based on deductive reasoning to policy analysis. This technique used on a logic-based specification of security policy with a clear semantic that leads to the analysis. This approach is not suitable for identifying causes of conflicts. Among the many approaches to policy specification and analysis, there are a number of proposals for formal, logic based notations. In particular, based on solid theoretical foundations [9], the authors in [2] proposed the use of Event Calculus as specialized first-order logic for formalizing policy specification.

Event Calculus uses familiar notations to specify the system behavior, which can be automatically translated into the logic program representation. Adductive reasoning proof procedures for Event Calculus [4] can be used to detect the existence of potential conflicts in partial specifications and generate explanations for the conditions under which such conflicts may arise.

Although this work offers a promising method to solve the problem of conflict analysis in a generic way, it is not sufficient to provide a complete solution to the problem without meet the needs of an application-specific domain.

VII. Conclusion

In this paper we have presented a formal characterization of security policy analysis, together with algorithmic solutions to policy analysis. To support automation of conflict detection for security policy, we first defined security conflicts in a formal way. Then, we developed mechanisms to systematically detect conflicts. Our work for policy analysis has been tested through the development of a prototype implementation. Next step is to extend our formalism to deal with policy refinement. This area need further work as policies are considered to exist at many different levels of abstraction and the transformation process from high-level policy to low-level implementable has remained a largely unresolved problem.

References

[1] R. J. Anderson. A security policy model for clinical information systems. In 1996 IEEE Symposium on Security and Privacy, pages 30–42. IEEE Computer Society Press,

[2] Bandara, E. Lupu, and A. Russo. Using event calculus to formalise policy specification and analysis. In 4th IEEE Workshop on Policies for Networks and Distributed Systems (Policy 2003), pages 26, 2003.

[3] N. C. Damianou. Policy Framework for the Management of Distributed Systems. PhD thesis, Imperial College. London, U. K., February 2002.

[4] M. Denecker and A. Kakas. Abduction in logic programming. Handbook of Logic in Artificial Intelligence and Logic Programming, 5:235–324, 1998.

[5] H. Hamdi, M. Mosbah, and A. Bouhoula. A domain specific language for securing distributed systems. In. ICSNC '07 Proceedings of the Second International Conference on Systems and Networks Communications Page 76, 2007.

[6] H. Hamdi, M. Mosbah, and A. Bouhoula. A declarative approach for easy specification and automated enforcement of security policy. International Journal os Computer Science and Networks, 8(2):60–71, Feb 2008.

[7] S. Jajodia, P. Samarati, and V. S. Subrahmanian. A logical language for expressing authorizations. In 18th IEEE Computer Society Symposium on Research in Security and Privacy, pages 31–42, 1997.

[8] L. Kagal, T. W. Finin, and A. Joshi. A policy based approach to security for the semantic web. In International Semantic Web Conference, pages 402–418, 2003.

[9] R. Kowalski and M. Sergot. logic-based calculus of events. New Generation Computing, 4:67–95, 1986.

[10] Lalana Kagal, Massimo Paolucci, Naveen Srinivasan, Grit Denker, Timothy W. Finin and Katia P. Sycara: Authorization and Privacy for Semantic Web Services. IEEE Intelligent Systems, pages 50-56, 2004.

[11] J. Lobo, R. Bhatia and S. Naqvi. A policy description language. In Proc. AAAI '99/IAAI '99, Pages 291-298 July, 1999.

[12] E. C. Lupu and M. Sloman. Conflicts in policy-based distributed systems management. IEEE Trans. Softw. Eng., 25(6):852–869, 1999.

[13] G. Wolfien. Network ipsec specification. In Pan-European Harmonisation of Vehicle Emergency call Service Chain.Information Society Technologies (IST), 25. October 2002.

 ISBN: 978-1-61208-231-8

Low-Complexity Lossless Compression on High-Speed Networks

Sergio De Agostino
Computer Science Department
Sapienza University
Rome, Italy
Email: deagostino@di.uniroma1.it

***Abstract*—We present a survey of results on how to implement low-complexity lossless data compression on a high speed network, so that the computational phase requires no interprocessor communication. It follows that the computation in between the input and output phases has a linear speed-up when the network size increases, regardless of the bandwidth and latency of the network. Depending on the type of data, the performance of the compression method changes in terms of scalability. Images are more suitable than strings, since text compression is scalable only on very large size files.**

Keywords-high speed network application; lossless compression; distributed algorithm; scalability.

I. INTRODUCTION

Arithmetic encoders enable the best lossless compressors by means of the model driven method [1]. The *model driven method* consists of two distinct and independent phases: *modeling* [2] and *coding* [3]. Arithmetic encoders are the best model driven compressors, but they are often ruled out because they are too complex. Low-complexity compression avoids arithmetic encoders.

Sliding window compression [4] is the most effective low-complexity text compression method (SW compression). When applied in parallel to data blocks on a large scale high speed network, the approach is practical only when the file size is large because of its adaptiveness [5].

Storer [6] extended SW compression to binary images by means of a square greedy matching technique (BLOCK MATCHING). The technique is suitable for high speed applications. Rectangle matching improves the compression performance, but it is slower since it requires $O(M \log M)$ time for a single match, where M is the size of the match [7]. Therefore, the sequential time to compress an image of size n by rectangle matching is $\Omega(n \log M)$. A variant of this method, called monochromatic pattern substitution (MP-SUB), compresses only monochromatic rectangles with a variable length code [8]. Such monochromatic rectangles are detected by means of a *raster* scan (row by row). If the 4 x 4 subarray in position (i, j) of the image is monochromatic, then we compute the largest monochromatic rectangle in that position else we leave it uncompressed. The encoding scheme is to precede each item with a flag field indicating whether there is a monochromatic rectangle or raw data. The procedure for computing the largest monochromatic rectangle with left upper corner in position (i, j) takes $O(M \log M)$ time, where M is the size of the rectangle. The positions covered by the detected rectangles are skipped in the linear scan of the image. The analysis of the running time of this algorithm involves a *waste factor*, defined as the average number of matches covering the same pixel. We experimented that the waste factor is less than 2 on realistic image data. Therefore, the heuristic takes $O(n \log M)$ time in practice. On the other hand, the decoding algorithm is linear. The compression effectiveness of this technique is about the same as the one of the rectangular block matching technique [7]. Moreover, compression via monochromatic pattern substitution (MP-SUB compression) has no relevant loss of effectiveness if the image is partitioned into up to a thousand blocks and each block is compressed independently. Therefore, the computational phase can be implemented on both small and large scale distributed systems with no interprocessor communication. BLOCK MATCHING, instead, does not work locally since it applies the generalized SW-type method with an unrestricted window. Finally, MP-SUB compression has a speed-up if applied sequentially to the partitioned image [9]. Experimental results suggest that the speed-up happens if the image is partitioned into up to 256 blocks and sequentially each block is compressed independently. It follows that the speed-up can also be applied to a parallel implementation on a small scale system. Such speed-up depends on the fact that monochromatic rectangles crossing boundaries between blocks are not computed and, consequently, the waste factor decreases when the number of blocks increases. If we refine the partition by splitting the blocks horizontally and vertically, after four refinements experimentations show that no further improvement is obtained.

The extension of Storer's method to grey scale and color images was left as an open problem, but it seems not feasible since the high cardinality of the alphabet causes an unpractical subexponential blow-up of the hash table used in the implementation. A low-complexity application compressing 8x8 blocks of a grey-scale or color image by

 ISBN: 978-1-61208-231-8

means of a header and a fixed-length code is presented in [10], which can be implemented on an arbitrarily large scale system with no interprocessor communication during the computational phase. A first step toward a good low-complexity compression scheme was FELICS (Fast Efficient Lossless Image Compression System) [11], which involves Golomb-Rice codes [12], [13]. With the same complexity level for compression (but with a 10 percent slower decompressor) LOCO-I (Low Complexity Lossless Compression for Images) [14] attains significantly better compression than FELICS. As explained in [10], parallel implementations of FELICS and LOCO-I require more sophisticated architectures than a simple array of processors.

As far as the model driven method for grey scale and color image compression is concerned, the modeling phase consists of three components: the determination of the context of the next pixel, the prediction of the next pixel and a probabilistic model for the *prediction residual*, which is the value difference between the actual pixel and the predicted one. In the coding phase, the prediction residuals are encoded. The use of prediction residuals for grey scale and color image compression relies on the fact that most of the times there are minimal variations of color in the neighborood of one pixel. Therefore, in [10] we were able to implement an extremely local procedure which is able to achieve a satisfying degree of compression by working independently on very small blocks. We presented the heuristic for grey scale images, but it can also be applied to color images by working on the different components. The main advantage is that it provides a highly parallelizable compressor and decompressor since it can be applied independently to each block of 8x8 pixels, achieving 80 percent of the compression obtained with LOCO-I (JPEG-LS), the current lossless standard in low-complexity applications. We called such procedure PALIC (Parallelizable Lossless Image Compression). The compressed form of each block employs a header and a fixed length code. Two different techniques might be applied to compress the block. One is the simple idea of reducing the alphabet size by looking at the values occurring in the block. The other one is to encode the difference between the pixel value and the smallest one in the block. This second technique can be interpreted in terms of the model driven method, where the block is the context, the smallest value is the prediction and the fixed length code encodes the prediction residual.

In Sections 2, 3 and 4, we explain the SW, MP-SUB and PALIC heuristics, respectively. The computational phase for these heuristics requires no interprocessor communication when implemented on a distributed system as, for example, a high speed network. It follows that the computation in between the input and output phases has a linear speed-up when the network size increases, regardless of the bandwidth and latency of the network. Quantitative results of such speed-up are provided in [5], [8], [9]. Conclusions and future work are given in Section 5.

II. Text Compression

Sliding window (SW) compression [4] is based on string factorization. Each factor extends by one character the longest match with a substring to its left in the input string. SW compression is a dictionary-based technique and is also called the sliding dictionary method. In fact, the factors of the string are substituted by *pointers* to copies stored in a dictionary. Distributed algorithms for SW compression approximating in practice its compression effectiveness have been realized in [5] on an array of processor with no interprocessor communication. However, the scalability of a parallel implementation of SW compression on a distributed system with low communication cost guarantees robustness only on very large size files.

A. SW Compression

Given an alphabet A and a string S in A^* the factorization of S is $S = f_1 f_2 \cdots f_i \cdots f_k$ where f_i is the shortest substring, which does not occur previously in the prefix $f_1 f_2 \cdots f_i$ for $1 \leq i \leq k$. With such factorization, the encoding of each factor leaves one character uncompressed. To avoid this, a different factorization was introduced where f_i is the longest match with a substring occurring in the prefix $f_1 f_2 \cdots f_i$ if $f_i \neq \lambda$, otherwise f_i is the alphabet character next to $f_1 f_2 \cdots f_{i-1}$ [15]. f_i is encoded by the pointer $q_i = (d_i, \ell_i)$, where d_i is the displacement back to the copy of the factor and ℓ_i is the length of the factor. If $d_i = 0$, l_i is the alphabet character. In other words a dictionary of factors is defined by a window sliding its right end over the input string, that is, it comprises all the substrings of the prefix read so far in the computation. The factorization processes just described are such that the number of different factors (that is, the dictionary size) grows with the string length. In practical implementations instead the dictionary size is bounded by a constant and the pointers have equal size. This can be simply obtained by bounding the match and window lengths (therefore, the left end of the window slides as well).

B. Compression with Finite Windows

A real-time implementation of compression with finite window is possible using a suffix tree data structure [16], [17]. Much simpler real-time implementations are realized by means of hashing techniques providing a specific position in the window where a good approximation of the longest match is found on realistic data. In [18], the three current characters are hashed to yield a pointer into the already compressed text. In [19], hashing of strings of all lengths is used to find a match. In both methods, collisions are resolved by overwriting. In [20], the two current characters are hashed and collisions are chained via an offset array. Also the Unix gzip compressor chains collisions, but hashes three characters [21].

 ISBN: 978-1-61208-231-8

C. The High Speed Network Implementation

For every integer k greater than 1 an O(kw) time, O(n/kw) processors distributed algorithm factorizing an input string S was presented on an array of processors with no interconnections in [5], whose cost approximates the cost of the string factorization within the multiplicative factor $(k+m-1)/k$, where n, m and w are the lengths of the input string, the longest factor and the window respectively. The approach provides an approximation scheme for such string factorization problem since the multiplicative approximation factor converges to 1 when kw converges to n.

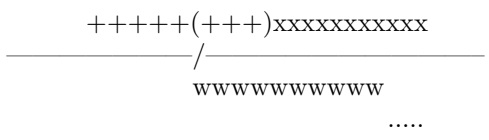


Figure 1. The making of the surplus factors.

We simply apply in parallel sliding window compression to blocks of length kw. It follows that the algorithm requires O(kw) time with n/kw processors and the multiplicative approximation factor is $(k+m-1))/k$ with respect to any parsing. In fact, the number of factors of a factorization on a block is at least kw/m while the number of factors of the factorization produced by the scheme is at most $(k-1)w/m+w$. As shown in Figure 1, the boundary might cut a factor (sequence of plus signs) and the length w of the initial full size window of the block (sequence of w's) is the upper bound to the factors produced by the scheme in it. Yet, the factor cut by the boundary might be followed by another factor (sequence of x's) which covers the remaining part of the initial window. If this second factor has a suffix to the right of the window, this suffix must be a factor of the sliding dictionary defined by it (dotted line) and the multiplicative approximation factor follows.

The approximation scheme is suitable for a small scale system but due to its adaptiveness it works on a large scale parallel system when the file size is large. From a practical point of view, we can apply something like the gzip procedure to a small number of input data blocks achieving a satisfying degree of compression effectiveness and obtaining the expected speed-up on a high speed network. Making the order of magnitude of the block length greater than the one of the window length largely beats the worst case bound on realistic data. The window length is usually several thousands of kilobytes. The compression tools of the Zip family, as the Unix command "gzip" for example, use a window size of at least 32K. It follows that the block length in our parallel implementation should be about 300K **at least. It follows that the file size should be at least about one third of the number of processors in megabytes.**

To decode the compressed files on the network, it is enough to use a special mark occurring in the sequence of pointers each time the coding of a block ends. The input phase distributes the subsequences of pointers coding each block among the processors.

III. Binary Image Compression

Monochromatic pattern substitution (MP-SUB) is so far the only low-complexity lossless binary image compression technique implementable on a high speed network with no interprocessor communication during the computational phase and no scalability issues [8]. We describe sequential and parallel implementations of this technique in the following subsections.

A. Monochromatic Pattern Substitution

The MP-SUB technique scans an image row by row. If the 4 x 4 subarray in position (i,j) of the image is monochromatic, then we compute the largest monochromatic rectangle in that position. We denote with $p_{i,j}$ the pixel in position (i,j). The procedure for finding the largest rectangle with left upper corner (i,j) is described in Figure 2. At the first step, the procedure computes the longest possible width for a monochromatic rectangle in (i,j) and stores the color in c. The rectangle 1 x ℓ computed at the first step is the current detected rectangle and the sizes of its sides are stored in $side1$ and $side2$. In order to check whether there is a better match than the current one, the longest sequence of consecutive pixels with color c is computed on the next row starting from column j. Its length is stored in the temporary variable $width$ and the temporary variable $length$ is increased by one. If the rectangle R whose sides have size $width$ and $length$ is greater than the current one, the current one is replaced by R. We iterate this operation on each row until the area of the current rectangle is greater or equal to the area of the longest feasible $width$-wide rectangle, since no further improvement would be possible at that point. Such procedure for computing the largest monochromatic rectangle in position (i,j) takes O($M \log M$) time, where M is the rectangle size. In fact, in the worst case a rectangle of size M could be detected on row i, a rectangle of size $M/2$ on row $i+1$, a rectangle of size $M/3$ on row $i+2$ and so on.

If the 4 x 4 subarray in position (i,j) of the image is not monochromatic, we do not expand it. The positions covered by the detected rectangles are skipped in the linear scan of the image. The encoding scheme for such rectangles uses a flag field indicating whether there is a monochromatic match (0 for the white ones and 10 for the black ones) or not (11). If the flag field is 11, it is followed by the sixteen bits of the 4 x 4 subarray (raw data). Otherwise, we bound by twelve the number of bits to encode either the width or the length of the monochromatic rectangle. We use either four or eight or twelve bits to encode one rectangle side. Therefore, nine

 ISBN: 978-1-61208-231-8

$c = p_{r,j}$;
$r = i$;
$width = m'$;
$length = 0$;
$side1 = side2 = area = 0$;
repeat
    Let $p_{r,j} \cdots p_{r,j+\ell-1}$ be the longest string in (r, j) with color c and $\ell \leq width$;
    $length = length + 1$;
    $width = \ell$;
    $r = r + 1$;
    if $(length * width > area)$ {
        $area = length * width$;
        $side1 = length$;
        $side2 = width$;
    }
until $area \geq width * (i - k + 1)$ or $p_{r,j} <> c$

Figure 2. Computing the largest monochromatic rectangle match in (i, j).

different kinds of rectangle are defined. A monochromatic rectangle is encoded in the following way:

- the flag field indicating the color;
- three or four bits encoding one of the nine kinds of rectangle;
- bits for the length and the width.

Four bits are used to indicate when twelve bits or eight and twelve bits are needed for the length and the width. This way of encoding rectangles plays a relevant role for the compression performance. In fact, it wastes four bits when twelve bits are required for the sides but saves four to twelve bits when four or eight bits suffice.

B. The High Speed Network Implementation

The MP-SUB technique has been applied to the CCITT test set (Figure 3) and has provided a compression ratio equal to 0.13 in average. The images of the CCITT test set are 1728 x 2376 pixels. If these images are partitioned into 4^k sub-images and the compression heuristic is applied independently to each sub-image, the compression effectiveness remains about the same for $1 \leq k \leq 5$ with a 1 percent loss for $k = 5$. Raw data are associated with the flag field 110, so that we can indicate with 111 the end of the encoding of a sub-image. For $k = 6$, the compression ratio is still just a few percentage points of the sequential one. This is because the sub-image is 27 x 37 pixels and it still captures the monochromatic rectangles which belong to the class encoded with four bits for each dimension. These rectangles are the most frequent and give the main contribution to the compression effectiveness. The compression effectiveness of the variable-length coding employed by the technique depends on the sub-image size rather than on the whole image. In fact, if we apply the parallel procedure to the test set of larger binary images as the 4096 x 4096 pixels half-tone

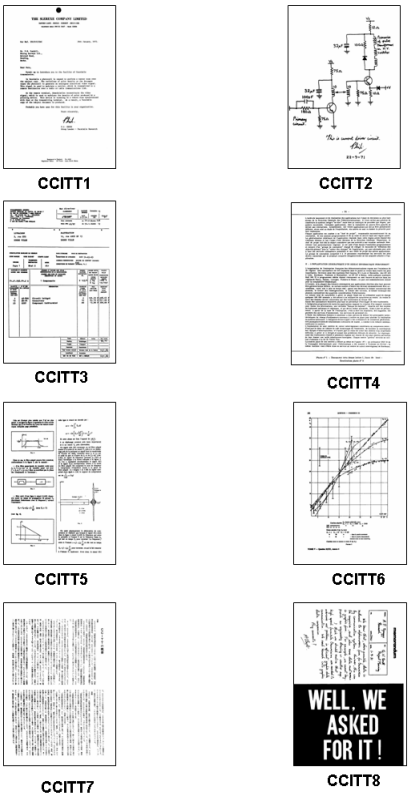


Figure 3. The CCITT image test set.

Figure 4. Images 1-5 from left to right.

topographic images of Figure 4, we obtain about the same compression effectiveness for $1 \leq k \leq 5$. The compression ratio is 0.28 with a 2 percent loss for $k = 6$. This means that actually the approach without interprocessor communication works in the context of unbounded parallelism as long as the elements of the image partition are large enough to capture the monochromatic rectangles encoded with four bits for each dimension.

C. A Sequential Speed-Up

We experimented that if we partition an image into 4^k sub-images and apply compression via monochromatic pattern substitution to each sub-image independently the waste factor decreases with the increasing of k [9]. A speed-up of the sequential algorithm follows from this fact. As mentioned in the introduction, the waste factor is less than 2 on realistic image data for $k = 0$ and decreases to about

1 when $k = 4$. It follows that if we refine the partition by splitting the blocks horizontally and vertically, after four refinements no further relevant speed-up is obtained. The same happens when we partition the set of 4096 x 4096 pixels images of Figure 4, that is, the waste factor seems to be determined by the number of refinements independently from the image size on realistic data. Obviously, there is a similar speed-up for the decompressor.

Since the sequential speed-up happens for an image partitioned into less than 256 blocks, it can be applied to a parallel implementation on a small scale network. Obviously, a similar experiment could be run using two refinemets or one refinement of the partition on a network of 16 or 64 nodes respectively.

IV. Grey Scale and Color Image Compression

We explain the PALIC heuristic which compresses grey scale and color images [10]. PALIC works independently on blocks of 8x8 pixels. The heuristic is described for grey scale images, but it can be trivially extended to RGB color images by working separately on each of the three components of the image. As previously mentioned, the compressed form of each block employs a header and a fixed length code.

A. The Heuristic

We still assume to read the image with a raster scan on each block. The heuristic applies at most three different ways of compressing the block and chooses the best one. The first one is the following.

The smallest pixel value is computed on the block. The header consists of three fields of 1 bit, 3 bits and 8 bits, respectively. The first bit is set to 1 to indicate that we compress a block of 64 pixels. This is because one of the three ways partitions the block in four sub-blocks of 16 pixels and compresses each of these smaller areas. The 3-bits field stores the minimum number of bits required to encode in binary the distance between the smallest pixel value and every other pixel value in the block. The 8-bits field stores the smallest pixel value. If the number of bits required to encode the distance, say k, is at most 5, then a code of fixed length k is used to encode the 64 pixels, by giving the difference between the pixel value and the smallest one in the block. To speed up the procedure, if k is less or equal to 2 the other ways are not tried because we reach a satisfying compression ratio on the block. The second and third ways are the following.

The second way is to detect all the different pixel values in the 8x8 block, to create a reduced alphabet and to encode each pixel in the block using a fixed length code for this alphabet. The employment of this technique is declared by setting the 1-bit field to 1 and the 3-bits field to 110. Then, an additional three bits field stores the reduced alphabet size d with an adjusted binary code in the range $2 \leq d \leq 9$. The last component of the header is the alphabet itself, a concatenation of d bytes. Then, a fixed length code is used for the 64 pixels.

The third way compresses the four 4x4 pixel sub-blocks. The 1-bit field is set to 0. Four fields follow the flag bit, one for each 4x4 block. The two previous techniques are applied to the blocks and the best one is chosen. If the first technique is applied to a block, the corresponding field stores values from 0 to 7 rather than from 0 to 5 as for the 8x8 block. If such value is in between 0 and 6, the field stores three bits. Otherwise, the three bits (111) are followed by three more. This is because 111 is used to denote the application of the second way to the block as well, which is less frequent to happen. In this case, the reduced alphabet size stored in these three additional bits has range from 2 to 7, it is encoded with an adjusted binary code from 000 to 101 and the alphabet follows. 110 denotes the application of the first technique with distances expressed in seven bits and 111 denotes that the block is not compressed. After the four fields, the compressed forms of the blocks follow, which are similar to the ones described for the 8x8 block. When the 8x8 block is not compressed, 111 follows the flag bit set to 1. How the heuristic works on an example is shown in [10].

B. The High Speed Network Implementation

The heuristic is obviously implementable on a large scale high speed network since an 8x8 pixels block is compressed independently. There is no issue in scaling down the network since one node can process more blocks sequentially [5]. On many images, we experimented positively the effectiveness of a less robust approach employing only the first way of compressing data, which shortens the coding and speeds up the process improving the compression efficiency.

C. Decompression

Parallel decoding of compressed gray scale images is trivial. As mentioned at the beginning of this section, color images are compressed by applying the method to each of the three components. It is obviously better to apply the method to each component of a block rather than coding each component of the whole image. In this way, besides producing on on-line decodable compressed form we simplify the input phase of the high speed network implementation.

V. Conclusion

We presented a survey describing three low-complexity lossless compression techniques for black and white images, color images and text respectively. These techniques can be implemented on a high speed network with no interprocessor communication. To garantee compression effectiveness and robustness, text compression requires each node of the network to store approximately 300 kilobytes of data while just 300 bytes suffice for black and white images. For color

 ISBN: 978-1-61208-231-8

images, it is even enough that a node stores 64 bytes. It follows that, as far as text compression is concerned, scaling up the network is possible only for very large size files. As future work, the design of a more local low-complexity text compression technique is the main goal.

REFERENCES

[1] T. C. Bell, J. G. Cleary, and I. H. Witten, *Text Compression,* Prentice Hall, 1990.

[2] J. Rissanen and G. G. Langdon, *Universal Modeling and Coding* IEEE Transactions on Information Theory 27, pp. 12-23, 1981.

[3] J. Rissanen, *Generalized Kraft Inequality and Arithmetic Coding* IBM Journal on Research and Development 20, pp. 198-203, 1976.

[4] A. Lempel and J. Ziv, *A Universal Algorithm for Sequential Data Compression,* IEEE Transactions on Information Theory 23, pp. 337-343, 1977.

[5] L. Cinque, S. De Agostino, and L. Lombardi, *Scalability and Communication in Parallel Low-Complexity Lossless Compression,* Mathematics in Computer Science 3, pp. 391-406, 2010.

[6] J. A. Storer, *Lossless Image Compression using Generalized LZ1-Type Methods* Proceedings IEEE Data Compression Conference, pp. 290-299, 1996.

[7] J. A. Storer and H. Helfgott H., *Lossless Image Compression by Block Matching* The Computer Journal 40, pp. 137-145, 1997.

[8] L. Cinque, S. De Agostino and L. Lombardi, *Binary Image Compression via Monochromatic Pattern Substitution: Effectiveness and Scalability* Proceedings Prague Stringology Conference, pp. 103-115, 2010.

[9] L. Cinque, S. De Agostino and L. Lombardi, *Binary Image Compression via Monochromatic Pattern Substitution: A Sequential Speed-Up* Proceedings Prague Stringology Conference, pp. 220-225, 2011.

[10] L. Cinque, S. De Agostino, F. Liberati and B. Westgeest, *A Simple Lossless Compression Heuristic for Grey Scale Images* International Journal of Foundations of Computer Science 16, pp. 1111-1119, 2005.

[11] P. G. Howard P. G. and J. S. Vitter, *Fast and Efficient Lossless Image Compression* IEEE Data Compression Conference, pp. 351-360, 1993.

[12] R. F. Rice, *Some Practical Universal Noiseless Coding Technique - part I* Technical Report JPL-79-22 Jet Propulsion Laboratory, Pasadena, California, USA, 1979.

[13] S. W. Golomb, *Run-Length Encodings* IEEE Transactions on Information Theory 12, pp. 399-401, 1966.

[14] M. J. Weimberger, G. Seroussi and G. Sapiro, *LOCO-I: A Low Complexity, Context Based, Lossless Image Compression Algorithm*, Proceedings IEEE Data Compression Conference, pp. 140-149, 1996.

[15] J. A. Storer and T. G. Szimansky, *Data Compression via Textual Substitution,* Journal of ACM 24, pp. 928-951, 1982.

[16] E. R. Fiala and D. H. Green, *Data Compression with Finite Windows,* Communications of ACM 32, pp. 490-505, 1988.

[17] E. M. Mc Creight, *A Space-Economical Suffix Tree Construction Algorithm,* Journal of ACM 23, pp. 262-272, 1976.

[18] J. R. Waterworth, *Data Compression System,* US Patent 4 701 745, 1987.

[19] R. P. Brent, *A Linear Algorithm for Data Compression,* Australian Computer Journal 19, pp. 64-68, 1987.

[20] D. A. Whiting, G. A. George, and G. E. Ivey, *Data Compression Apparatus and Method,* US Patent 5016009, 1991.

[21] J. Gailly and M. Adler, http://www.gzip.org, 1991 [retrieved: October, 2012].

 ISBN: 978-1-61208-231-8

1 Gbps Ethernet TCP/IP and UDP/IP Header Compression in FPGA

Milan Štohanzl, Zbyněk Fedra
Department of Radio Electronics
Faculty of Electrical Engineering and Communication
Brno University of Technology
Brno, Czech Republic
e-mail: stohanzl@phd.feec.vutbr.cz,
fedraz@feec.vutbr.cz

Marek Bobula
Research and Development Department
Racom Ltd.
Nové město na Moravě, Czech Republic
marek.bobula@racom.eu

***Abstract* — This paper presents a study about the hardware implementation of the TCP/IP and UDP/IP headers compression for the point-to-point communication. The implementation is focused on the achievement of minimum latency and high compression ratio. The applied compression technique is a dictionary-based method. For the TCP/IP, the fixed length of the compressed header was implemented. On the contrary, the variable length of the compressed header was implemented for the UDP/IP. The dictionaries are filled from the original data on both sides. No additional transmissions are used for retaining the continuity of the dictionary content.**

Keywords-Field Programable Gate Array (FPGA); Ethernet; header; compression; connection; IP; TCP; UDP.

I. INTRODUCTION

In order to reduce the amount of transmitted data over physical layer of the IP network, lossless data compression can be implemented. This can be useful for the one hop of the point-to-point radio or optical Ethernet link especially for solution integrated with a modem. The lossless data compression is used for reducing the data redundancy at the transmitter side (in a compressor). This redundancy is renewable at the receiver side (in a decompressor). In general, the random character of the Ethernet data traffic must be considered [2]. For this reason, any lossless data compression method may fail as the statistical-based and dictionary-based lossless data compression methods are based on the data redundancy (with specific sequence and/or time dependency). Statistical-based compression methods are unsuitable more than dictionary based methods because they need more time for preprocessing (creation of data statistics) [1]. However, the character of data in the headers of data link layer, network layer and transport layer is well known and/or predictable [6] [7] [8].

The data cannot be transferred trough IP networks without headers [9]. The second, the third and the fourth layers add the headers to the data. These headers are used for routing and transferring data through network. A single TCP connection or UDP data flow is usually hundreds or thousands of packets transmitted from source to destination. There are a lot of data that do not change during the connection in headers TCP/IP connection or UDP/IP flow. Repeated transfers of headers add the redundancy (unchanging data in headers) or the redundancy in long numbers transmitting which are changed only minimally packet by packet. Such items can be transferred in the form of differences. The main idea of the header compression is in the replacement of long raw headers by headers without redundancy. The original headers are identically restored at the receiver side [1] [2] [4].

The length of original headers is strictly defined, or is defined in some extent [6] [8]. On the contrary, the length of transmitted payload is entirely random. The headers may take up to 50 % of the volume of the transmitted data at the physical layer (when a very short payload is transmitted). When the frames over the MTU (Maximum Transmission Unit) (1500 B) are transmitted the headers take less than 5 % of volume transported on physical layer.

There are two general ways of implementing a compression algorithm. Software implementation is costs effective for low speed connections. For real-time applications with high speed connections, hardware implementation is better. Nowadays, the compression hardware exists in many forms, for example Lempel-Ziv algorithms [2], X-Match Pro Algorithms [3] and many more. The information about hardware implementation specialized in the Ethernet headers compression was not found. The software implementation of the TCP/IP headers compression was designed and published in RFC 1144 [4] and RFC 2507 [5]. Therefore, this study deals with hardware implementation of the Ethernet headers compression (TCP/IP and UDP/IP).

This paper is divided into eight sections. The original headers and compressed headers formats are introduced in Section II. Section III describes the applied method. The hardware arrangement is presented in Section IV. The compressor is discussed in Section V and the differences between compressor and decompressor are discussed in Section VI. The results of this research are summarized in Section VII. The conclusion of the present study can be found in Section VIII.

II. ORIGINAL AND COMPRESSED HEADERS

In this section, the original and compressed headers content and its meaning is described.

The IP header format is shown in Figure 7. IP version is a four-bit item. The IP length is a four-bit item and it represents one quarter of the total IP length. The basic length

 ISBN: 978-1-61208-231-8

of an IP header is 20 bytes. All the IP headers with different lengths are not compressed. The item ToS (Type of Services) contains the Differentiated Services Codepoint and the Explicit Congestion Notification. One of the compression conditions is the ToS equal to zero. The total IP length is the length of the IP packet. It is a sum of the IP header length, the higher layer protocol header length and the data (payload) length. This item is transmitted in the compressed header without any changes. IP Identification (IP ID) is the number of IP packets sent by the station. The IP ID in the TCP/IP stream is changed only minimally being sent packet by packet and therefore it is transmitted in the compressed header as an eight-bit difference. The field flags and the fragment offset are set only when the IP packet is fragmented. This field must be zero (compression condition). Only the DF (Don't Fragment) bit can be written to one. In this case, the seventh bit in the compressed header is set to one. The TTL (Time To Live) is a number that limits the lifespan of the IP packets in the IP networks. This value is constant for one TCP/IP stream at one line (when the IP packets are routed by the same way trough the IP network). The item protocol identifies higher layer protocol. For example TCP is presented by number 6, UDP is presented by number 17. The IP checksum is the checksum of all bytes in the IP header. This value need not be transmitted in the compressed header and can be evaluated during the decompression process. As a result, however, the error protection would be decreased. This value is transmitted in the compressed header without any changes. The source and destination IP addresses are the IP addresses of the end nodes and they identify the TCP/IP data stream and/or the UDP/IP data flow. [6]

The basic length of the TCP header is 20 bytes. The source and destination ports together with the IP addresses identify the TCP/IP data stream. The Sequence Number (SEQ) and the Acknowledgement Number (ACK) are changing (increasing) in TCP/IP stream packet by packet. Therefore they are transmitted in compressed header as a 16-bit difference. The data offset represents the length of the TCP header. The implemented compression algorithm allows the compression of the TCP headers with basic length. The TCP flags field contains the TCP flags. Only the headers with a set Acknowledgement flag can be compressed. If the Push flag (PSH) is set, compression is allowed and the eighth bit in the compressed header is set to one. Other flags (Urgent, Reset, Syn, Fin) must not be set. The Window size value is transmitted in the compressed header without any changes. The TCP checksum is the checksum of all bytes in the TCP header and the data payload. The evaluation of this checksum during the decompression process would cause the decrease of the error protection in a similar way as with the IP checksum. Moreover, the whole TCP packet including the payload would have to be buffered. This would disproportionately increase the latency. Therefore, the TCP checksum is transmitted in the compressed header without any changes.The urgent pointer is only set if the urgent flag is set to one. Therefore the urgent pointer is not transmitted in the compressed header. The original TCP header format is shown in Figure 8 [8].

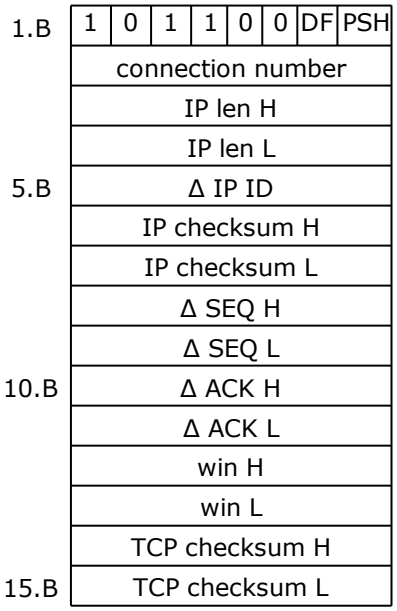


Figure 1. Compressed header format (TCP/IP).

The UDP header consists of eight bytes. Four bytes are port numbers. The item UDP length is the length of payload and the UDP header. This item can be calculated by subtracting the IP header length of the (20 B) from the IP length. The UDP checksum is the checksum of all bytes in the payload and the UDP header. This item is transmitted in the compressed header. The original headers format is shown in Figure 8. In Figure 2, the formats of the compressed UDP/IP headers are shown. As can be seen, the length of the header is variable. The item IP ID is not included in the compressed header when the IP ID is zero in the original data flow. The Δ IP ID is transmitted in when the difference between the previous and the current value is less or equal to the eight-byte-value. Otherwise, the IP ID is transmitted without changes. The format of the compressed header is indicated by the seventh and the eighth bit in the compressed header. The compressed UDP/IP header formats are shown in Figure 2 [7].

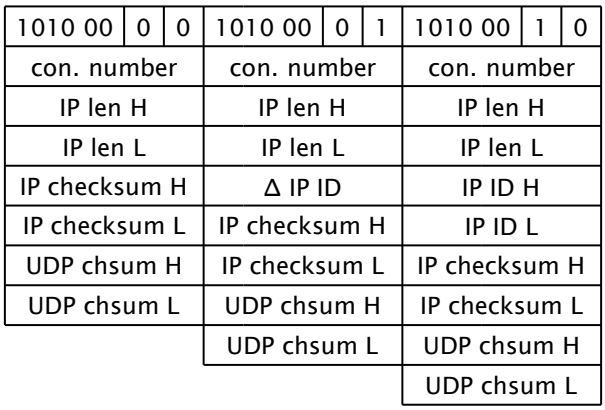


Figure 2. Compressed header formats (UDP/IP).

III. METHOD

The implemented header compression technique is a dictionary method. The compressor and decompressor dictionaries contain data from raw (original) headers that are transmitted in the compressed headers as the difference or are not transmitted in the compressed headers at all. The dictionaries are divided into cells. Every cell contains data for one TCP/IP or UDP/IP flow. The width of the words in a cell is defined for each word separately. Each cell also contains the "connection number" item and the "Counter of Use" (CoU). The CoU is used to detect the flow inactivity (see below).

At the beginning (after start-up), the compressor and decompressor dictionaries are empty. With the arrival of the first packet that meets the conditions of the compression, the raw data from headers are stored in one dictionary cell. The packet is sent without any changes. At the receiver side, the decompressor identifies this compressible packet and stores the raw data in one cell as does the compressor. After the arrival of the next packet of this flow, the compressor finds a match in the dictionary and compresses the headers. During the compression process, the compressor actualizes data in the cell from the raw headers (only changing data like IP ID, ACK, SEQ that are transmitted like differences) and increments the CoU. The decompressor detects the compressed header and decompresses this header using the data from dictionary in the same way the compressor actualizes data in the dictionary and increments the CoU at the decompressor side. Described procedure ensures that the compressor and the decompressor have the same content of dictionary at all times. This is the main condition of this method.

When the compressor finds a match in the dictionary but the raw headers are not compressible (a difference is greater than one byte and/or the flags in raw headers do not allow compression), the raw data are transmitted and the compressor/decompressor actualizes the data in the dictionary. There is a chance that the next packet of this flow will be compressible.

When all the cells of the dictionary are full and the compressor identifies compressible packet without a match in the dictionary, a revision of the dictionary is made. All cells with the CoU equal to zero (only one packet of the flow which allowed the compression passed) are released. For easier implementation, the packet is transmitted without any changes and is not stored in the dictionary. The decompressor does the same. It is also possible for the CoU in all cells not to be equal zero. In this case, the "Counter of Raw Data" (CoRD) is incremented. If the CoRD is equal to the pre-set threshold every CoU is reset. Subsequently, the packets from the stored flows may come. These packets are compressed and the CoUs in the cells of the dictionary are incremented. The first compressible packet which is not in the dictionary causes the release of cells with the CoU equal to zero. The method of zeroing CoU in case of full dictionary and transmitting unstored flows guarantees the old data in the dictionary are cleared and the dictionary is ready for the current flows. The data in the dictionary will never grow so old so as to render the storing of new data impossible.

IV. HW SOURCES

The data rate 1 Gbps (Ethernet IEEE 802.3z) corresponds to modulation rate 1.25 GBaud on the physical layer. After the deserializer, the data rate on GMII busses between MAC/PHY (Media Access Control, Physical Layer) circuits and the FPGA in Figure 3. is 125 Mbit/s. The main clock in the FPGA is the same (125 MHz corresponds to 8 ns). The hardware arrangement is presented in Figure 3. The GMII bus contains eight wires for the data, one wire for clock signal and one wire for validation signal.

The original signal from the Ethernet line is modified in the MAC/PHY circuit and brought into the FPGA. The modification (header compression) can be performed there. Then the data flow is connected to the second PHY/MAC circuit. This circuit must not monitor the CRC (Cyclic Redundancy Check) of the Ethernet frame and the headers content. The decompression must be implemented from the second side. The TX/RX (Transmit, Receive) line is ideal (without losses and interferences).

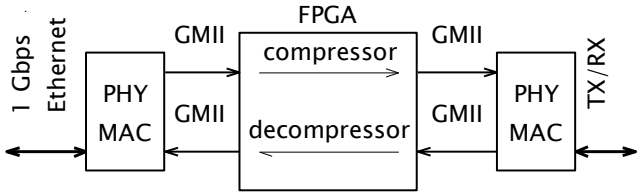


Figure 3. HW arrangement.

V. THE COMPRESSOR

The compressor processes (as well as the decompressor processes) are divided into three basic blocks. These blocks are shown schematically in Figure 4. The first block recognizes the header items of the TCP/IP and UDP/IP, in the second block the data flow is delayed in order to allow the third block to evaluate the header items before it starts to process or compress them in the original data flow.

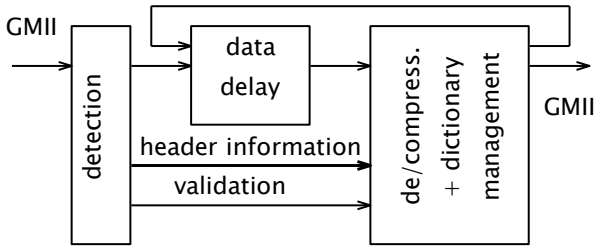


Figure 4. Block diagram of the de/compressor.

A. Detection

The main task of the header detector is to identify the header items from the TCP/IP and UDP/IP headers. This header information is copied on parallel busses. After the

stabilization of the data in the busses, the single-bit validation signal is set. The validation of the parallel data is necessary because the data are set to the busses byte by byte but the bus(ess) width corresponds to the word width of the current information item. The example of parallel bus setting is shown in Figure 9. The detection process is realized by the combinational state machine which secures the content and the order of the data in the Ethernet frame, shown in Figure 6. The byte order is determined by the internal counter of bytes. This counter is activated or reset by the validation signal of the GMII bus.

The example of the VHDL (Very High Speed Integrated Hardware Description Language) code from detector follows. There are four states from combinational state machine shown when the source IP address is detected. One-bit combinational variable the "Comb_ip_source" is set to one in these states. In other states, it is set to zero.

```
When st_sniff_IP_12 =>
        Comb_ip_source <= '1';
        Next_State_sniff <= st_sniff_IP_13;
When st_sniff_IP_13 =>
        Comb_ip_source <= '1';
        Next_State_sniff <= st_sniff_IP_14;
When st_sniff_IP_14 =>
        Comb_ip_source <= '1';
        Next_State_sniff <= st_sniff_IP_15;
When st_sniff_IP_15 =>
        Comb_ip_source <= '1';
        Next_State_sniff <= st_sniff_IP_16;
```

The variable "Comb_ip_source" is tested in the sequential part. The vectors "Loc_ip_src_N" and "data_inner" are eight-bit vectors. The "data_inner" contains the current data byte of the data flow.

```
If Comb_ip_source = '1' then
        Loc_ip_src _0 <= data_inner;
        Loc_ip_src _1 <= Loc_ip_src _0;
        Loc_ip_src _2 <= Loc_ip_src _1;
        Loc_ip_src _3 <= Loc_ip_src _2;
End if;

IP_SOURCE_OUT <= (Loc_ip_src_3 & Loc_ip_src_2
& Loc_ip_src_1 & Loc_ip_src_0);
```

The last line of the example is the combinational output. "IP_SOURCE_OUT" is 32-bits output vector. An example of the filling of this vector is presented in Figure 9. This example was taken by the JTAG (Joint Test Action Group) from the FPGA. Each vector is in hexadecimal format. The first line of this example shows the vector-data IP_SOURCE_OUT, the second line shows the IP_DEST_OUT (destination IP address). The third line shows the data_inner and the last line shows the states of the state machine. As can be seen, the state "st_sniff_IP_12" corresponds to 23_h. The byte 93_h (147_{10}) is the highest byte of the source IP address. This byte affects the value of the output vector in the next clock cycle. Every byte of the source IP address is gradually processed in the same way. The vector "IP_SOURCE_OUT" is valid in the state 27_h. Then, the following data are processed in a similar way (destination IP address,...). A validation signal is set at the moment when all data at all parallel buses are valid.

B. Data delay

There are several ways of creating a delay in the data stream in FPGA. A long shift register is easy to implement in VHDL, but it is very demanding for hardware resource consumption. A FIFO (First In First Out) memory allows reading the data flow with the delay but this delay can not be changed during the reading process. On the contrary, a RAM (Random Access Memory) memory allows the reading from any address. For this reason, the delay is implemented by the RAM memory and it is driven by the special driver (written in VHDL). The RAM memory is implemented as soft IP core and uses memory blocks of the FPGA. It is the Simple Dual-port RAM [10] with 128 word depth (every word is one byte). Every incoming byte is written in the RAM and the writing address (controlled by the RAM controller) is incremented. The data reading from RAM starts when writing address exceeds some threshold. The change of the delay is initialized by the third block (compressor). It is shown by the feedback from the third block to the delay block in Figure 4. The connection between RAM and RAM driver is shown in Figure 5. (WR means writing and RD means reading).

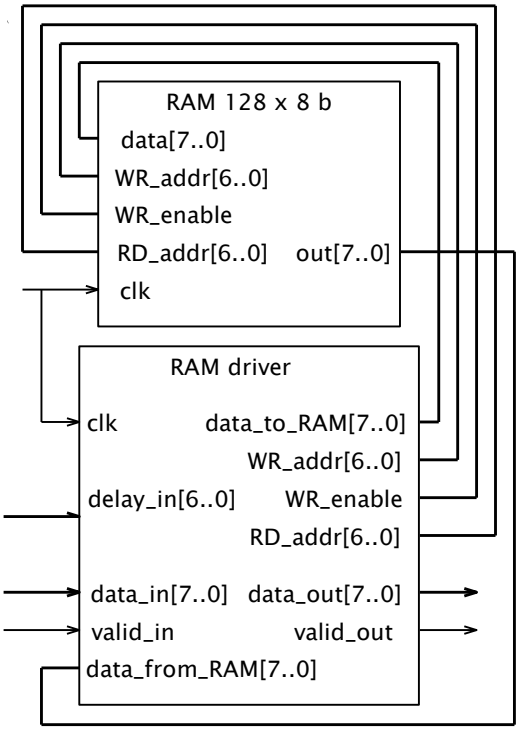


Figure 5. Delay block interconnection.

There is a delay between the writing of reading address and getting the data from the RAM output. This delay is

caused by the gating signals in RAM memory at inputs and outputs (two clock periods) and the actual reading process (one clock period). For this reason, the reading data from RAM memory are connected to the RAM driver and they are supplemented by the correct validation signal.

C. Compressor and dictionary management

The compressor block also performs the dictionary management, as was described in Section III. The compressor evaluates the original header data from the parallel busses and decides whether they meet the compression conditions, finds a match in the dictionary, compress header and/or actualizes the dictionary. The dictionary is also actualized when the match in the dictionary is found while the original header did not meet the compression conditions.

A function of the compressor is controlled by the combinational state machine, the calculations are included in the sequential part. While the compression is running, the original headers (IP, TCP and UDP) are replaced by the compressed header. The data (payload) immediately follow the compressed header. The length of the compressed header is shorter than the original headers. It means that the delay of the data flow must be changed during the compression process. In a design with the variable length of the compressed header the change of the delay must be variable. For this reason, the vector "delay_in" has the same length as the reading address "RD_addr". The value of delay change is added to the reading address value. The example is in Figure 10. The reading address is in the first line, the second line shows the validation signal, the third line shows the reading data from RAM. The last line shows the "delay_in" vector. This vector is set to zero and contains the value 19_h (25_{10}) only in one clock tact. In the next clock tact, the reading address is changed from 24_h to $3E_h$. The value of the reading address is increased by one (in every clock pulse) plus extra 19h. As described above, the output data from the RAM are delayed by three tacts following the reading address. The bytes 47_h, 45_h and 54_h in the data flow are ASCII symbols 'G', 'E' and 'T'. It is the start sequence of payload in packet (access to the web). The byte 00_h in the data flow before this sequence is caused by the change of the reading address. Nevertheless, this error is of no importance as this byte as well as the preceding bytes are replaced by the compressed header.

The example of the header compression is shown in Figure 11. In the first line internal byte counter is shown, the "delay_in" is shown in the second line. The original data flow at the input of the compressor is shown in the third line. The sequence starts by the start of the IP header. The IP length is 0024_h, IP ID is $07B7_h$ and TTL is 80_h. The payload immediately follows the TTL (the change of the delay is reflected). The payload sequence means "Hello." in ASCII. In the last line of the example, the output data flow with the UDP/IP compressed header is shown. The first byte is $A1_h$, it presents format with Δ IP ID (01_h). Connection number is 63_h.

VI. THE DECOMPRESSOR

The decompressor is divided into three blocks like the compressor. These blocks are similar to the blocks at the compressor side. The differences between the two are described bellow.

A. Detection

The detector at the decompressor side allows the detection of the compressed headers. The parallel busses between the detector and the decompressor include wires for items from the compressed headers.

B. Data delay

The delay of the data flow is realized in a similar way as at the compressor side. The difference is only in the sign for "delay_in" vector. During the decompression process, the delay must increase because the length of the recovered headers is larger than the length of the compressed header.

C. Decompressor and dictionary management

The dictionary management at the decompressor side is the same as that at the compressor side. The decompressor (like the compressor) searches matches in the dictionary and performs the basic dictionary tasks (storing data, actualizing data, releasing cells,...).

When the decompressor processes the data from the compressed header, it seeks consensus by the connection number in the dictionary. Then, the decompressor calculates original header items from the dictionary data and the received differences, actualizes the dictionary and stores the recovered header items in the internal vectors. These data are put in the output data flow in the correct order (controlled by the internal byte counter in sequential part. The restored header must be closely followed by the payload and therefore the delay is changed during this process.

VII. RESULTS

The described header-compressor and decompressor were implemented in FPGA Altera Cyclone III, namely the EP3C40F484C7 with speed grade -8, 39,600 Logic Elements (LE), more than 1 Mbits Random Access Memory, 126 M9K (special memory) blocks, 126 multipliers (18 x 18), four PLLs (Phase Locked Loop [11].

The TABLE I. contains the FPGA synthesis result. The compressor and decompressor dictionaries have five cells for the TCP/IP streams and five cells for the UDP/IP flows. The decompressor detector is more demanding on hardware resources than the compressor detector for its ability of detection also of the compressed headers. The decompressor calculates original header items and stores them in the internal vectors in contrast with the compressor which put the compressed header data directly into the output data flow. Therefore, the decompressor implementation is more hardware demanding. The difference between the data delay blocks at the compressor and decompressor sides is very simple (see in Section VI). Nevertheless, the consumption of the LEs and LUTs is higher at the decompressor side.

 ISBN: 978-1-61208-231-8

TABLE I. REQUIRED HW SOURCES

		LEs	M9Ks	LUTs
Compressor	***Detector***	404	0	109
	Data delay	74	1	24
	Compressor	3661	0	1635
Decompressor	***Detector***	526	0	156
	Data delay	82	1	32
	Decompressor	4240	0	1760

The above described implementation allows the compression of TCP/IP and UDP/IP headers with the compression from 40 to 15 bytes for TCP/IP and from 28 to 8, 9 or 10 bytes for UDP/IP. This compression and decompression processes were designed with respect to minimum delay in the data flow, in contrast to the systems that perform the compression of the headers after the buffering the whole packet. The delay is variable for Ethernet frames with compression while the delay is constant for the frames without compression. In the worst case, the flow delay is less than 50 clock periods at the compressor side and less than 30 clock periods at the decompressor side. It is less than 640 ns.

VIII. CONCLUSION

The paper presented the implementation of the header compressor for one Gbps Ethernet in the FPGA. The compression and decompression of the TCP/IP and UDP/IP headers in presented form was implemented and tested.

The variable length format of the compressed header for the TCP/IP and IPv6 header compression will also be incorporated. The future work would also include mechanisms for handshaking between the compressor and the decompressor dictionaries and for the data protection. These mechanisms would allow the use of the TX/RX real line (with losses and interferences). However, these mechanisms should be implemented on the lowest layer. It would require implementation of the MAC/PHY into FPGA.

ACKNOWLEDGMENT

This paper was supported by the project Systems of Wireless Internet Communication (SYWIC) LD11081 in frame of COST IC 0906 action. The research published in this submission was financially supported by the project CZ.1.07/2.2.00/20.0007 WICOMT of the operational program Education for competitiveness and by grant no. FEKT-S-11-12 (MOBYS).

The described research was performed in laboratories supported by the SIX project; the registration number CZ.1.05/2.1.00/03.0072, the operational program Research and Development for Innovation.

REFERENCES

[1] D. Salomon and G. Motta, Handbook of Data Compression, Springer-Verlag, London, 2010.

[2] R. Mehboob, S. A. Khan, and Z. Ahmed, "High speed lossles data compression architecture," Multitopic Conference, 2006. INMIC '06. IEEE, pp. 84-88, 23-24 Dec. 2006, doi: 10.1109/INMIC.2006.358141.

[3] J.L. Nunez-Yanez and V.A. Chouliaras, "Gigabyte per second streaming lossless data compression hardware based on a configurable variable-geometry CAM dictionary," Computers and Digital Techniques, IEE Proceedings, vol. 153, no. 1, pp. 47-58, 10 Jan. 2006, doi: 10.1049/ip-cdt:20045130.

[4] V. Jacobson, B. Nordgren and S. Pink "Compressing TCP/IP headers for low-speed serial links," RFC 1144, Feb. 1990.

[5] M. Degermark, "IP header compression," RFC 2507, Feb. 1999.

[6] "Internet protocol DARPA internet program protocol specification," RFC 791, Sep. 1981.

[7] J. Postel, "User Datagram protocol," RFC 768, Aug. 1980.

[8] "Transmission Control Protocol," RFC 793, Sep. 1981.

[9] "IEEE 802.3. Part 3: Carrier sense multiple access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications," New York: IEEE Computer Society, pp. 49 2008.

[10] www.altera.com, "Internal memory (RAM a ROM) User Guide," Jan. 2012

[11] www.altera.com, "Cyclone III Device Family Overview," vol. 1. 2012.

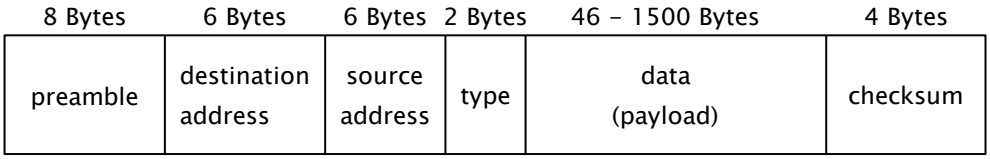


Figure 6. Ethernet frame (Ethernet II). [9]

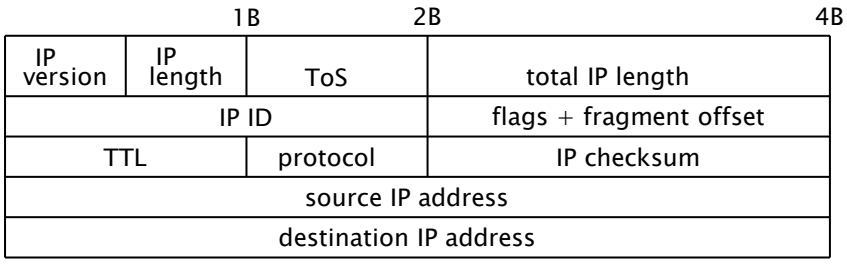


Figure 7. IP header (IPv4). [6]

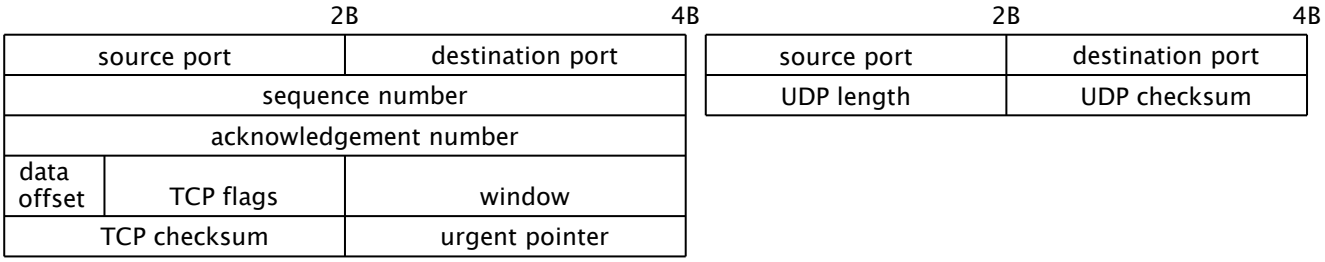


Figure 8. TCP header format (left), UDP header format (right). [7] [8]

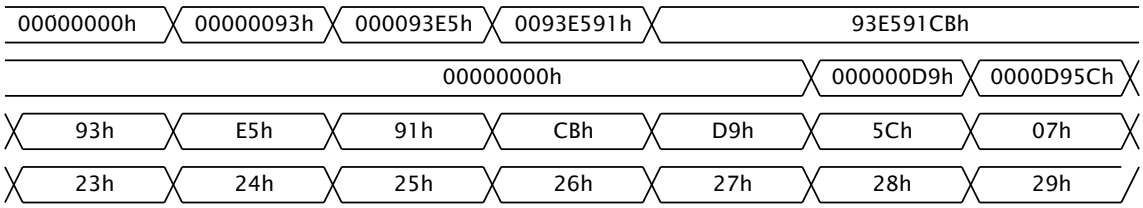


Figure 9. The example of filling of the “IP_SOURCE_OUT” data vector.

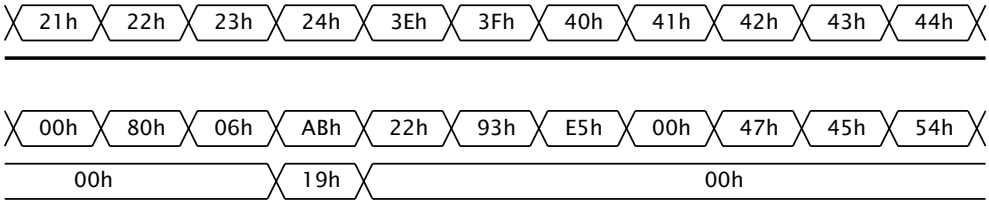


Figure 10. The example of changing of the reading address.

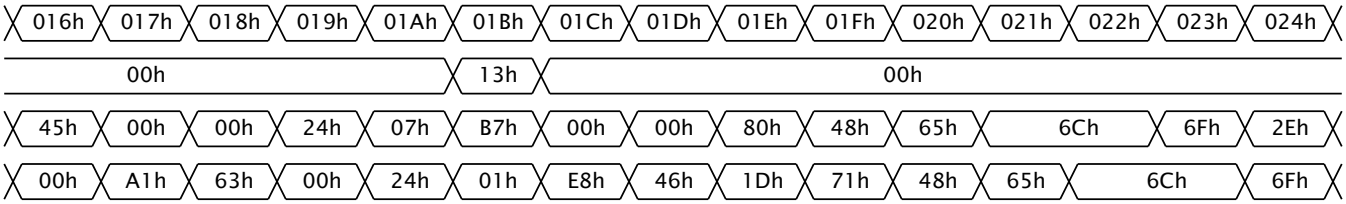


Figure 11. UDP header compression.

 ISBN: 978-1-61208-231-8

Best Shortest Lightpath Routing for Translucent Optical Networks

Gilvan M. Durães
Optical Networks Group
Baiano Federal Institute of Education, Science and Technology, Catu, Brazil
gilvan.duraes@catu.ifbaiano.edu.br

André C. B. Soares
Department of Informatics and Statistics
Federal University of Piauí – UFPI
Teresina, Brazil
andre.soares@ufpi.br

William F. Giozza
Department of Electrical Engineering
University of Brasília – UnB
Brasília, Brazil
giozza@unb.br

José Augusto Suruagy Monteiro
Federal University of Pernambuco – UFPE
Informatics Center (CIn)
Recife, Brazil
suruagy@cin.ufpe.br

***Abstract*—This work extends for translucent optical networks the solution to the problem of finding the best choice among *M* combinations of the shortest paths. The proposed Best Shortest Translucent Lightpath (BSTL) is a novel optical routing strategy, adaptive and aware of the optical physical layer impairments. The performance of BSTL is evaluated at different scenarios (topologies, regenerator placements, impairment thresholds, etc.) using metrics like network utilization, blocking probability, and fairness. In all these scenarios, BSTL achieved a better performance that related algorithms, such as PIARA.**

Keywords – Translucent Optical Networks; Optical Physical Layer Impairment-aware Routing; Performance Evaluation.

I. INTRODUCTION

Optical networks are currently based on the Wavelength Division Multiplexing (WDM) [1] technology. WDM allows the establishment of various optical circuits (lightpaths) simultaneously in a single optical fiber using different wavelengths.

The architecture of an optical network can be classified as opaque, transparent or translucent [1]. In opaque optical networks, all nodes are opaque, i.e., each node requires Optic-Electrical-Optical (OEO) conversions of optical signals from input ports to electrical signals before processing and forwarding to output ports where electrical signals are reconverted to optical signals in order to be transmitted. Opaque nodes allow the regeneration of optical signals but the use of OEO converters insert unnecessary delays and are quite expensive. On the contrary, in transparent optical networks there are no OEO conversions at intermediate nodes of a route. In this case, optical signals are processed exclusively in the optical domain through all-optical switches. Therefore, transparent optical networks eliminate signal conversion delays at intermediate nodes of a route. In translucent optical networks, which use a hybrid approach, there are some nodes with OEO conversion capability and all others are transparent. This allows the regeneration of the optical signal along specific routes.

In practice, an optical signal is impaired when propagating through optical fiber links, optical cross-connects, optical amplifiers and other optical network elements. The accumulation of these impairments along a route, tends to increase the Bit Error Rate (BER) at the receiver, reaching prohibitive levels [2,3]. Currently, optical technologies impose the need of OEO conversions in long distance routes in order to mitigate impairments at some intermediate nodes [2]. Therefore, a new optical network architecture that uses OEO conversions at some intermediate nodes and all-optical switching in all other nodes has to be considered. Gathering features like fast switching from transparent optical networking and signal regeneration from opaque optical networking, translucent optical networking became a reality [2,3]. In this work, translucent optical networks, where opaque nodes are sparsely distributed in the network topology, is considered. Also, it is assumed the circuit-switched optical networking paradigm which means that an optical circuit (transparent or translucent lightpath) is dynamically established using network resources (wavelengths) along a route (links and nodes) between a pair of source and destination nodes.

The lightpath routing problem in circuit-switched optical networks is also known as Routing and Wavelength Assignment (RWA) [4]. RWA routing algorithms can be separated in three classes: fixed routing, alternate routing, and exhaustive routing [4].

In the fixed routing strategy, each pair of nodes (source, destination) has only one route that is previously computed. Therefore, even before a lightpath request arrival, the routing control plane already knows which route must be used for a specific source-destination pair. Normally, fixed routes are previously computed using a classical shortest path algorithm, like Dijkstra's algorithm [5] or other routing algorithms specially proposed for optical networks [6, 7, 8].

In the alternate routing strategy, a set with more than one route is previously defined for each source-destination pair. Alternate routing can be classified as fixed-alternate or adaptive alternate routing. Their differences lie in the way of selecting one route from the pre-computed set of routes. In fixed-alternate routing [4,8], the sequence of routes is

 ISBN: 978-1-61208-231-8

previously defined. Routes are tried one by one in a predetermined order to establish a lightpath for a specific request. In case of failure, the lightpath request is said to be blocked. In adaptive alternate routing or adaptive routing for short [4], route selection from the pre-computed set of routes is based on the network current state. For example, one may select the least loaded route.

The exhaustive routing class algorithms have the advantage of being able to select any possible route in the topology for establishing a lightpath [4]. Therefore, in this case, a lightpath request will be blocked only if there are no routes between source and destination with at least one available continuous wavelength. However, the implementation of exhaustive routing algorithms is more complex than the implementations of the other routing classes.

This work presents a new adaptive routing algorithm for translucent optical networks, named Best Shortest Translucent Lightpath (BSTL). BSTL is inspired on the Best among Shortest Routes (BSR) proposal which optimizes the fixed routing problem in transparent optical networks [6]. But, differently from BSR, BSTL is adaptive and aware of optical physical layer impairments.

The optical physical layer impairment-aware dynamic routing problem in translucent optical networks is considered more difficult than the corresponding problem for transparent optical networks [9]. Optical physical layer impairments can be classified in two categories: linear and nonlinear. Linear impairments are independent of the optical signal power and affect each of the wavelengths individually, while the nonlinear impairments scale with optical power, affecting all wavelengths. The main linear impairments such as fiber attenuation, insertion loss, amplifier spontaneous emission, dispersion and crosstalk, are already well characterized [10]. On the other side, nonlinear impairments are more complex and difficult to characterize, needing a detailed knowledge of the optical network infrastructure. However, it is possible to adopt a simplified model where nonlinear effects are mitigated by minimizing the number of links along the lightpath [11].

Most optical signal impairments occur in function of the distance and/or the number of intermediate switches involved in the path from the source to the destination node. In this work, it is considered a hop number limit for a route without optical signal regeneration. Therefore, a lightpath must have optical signal regeneration (translucent lightpath) when it reaches a specific hop number, known as Impairment Threshold (IT) [8]. Several works in the literature adopt the hop number limitation as the main optical signal quality measure for performance evaluation of translucent optical networks [2,3,8,10,12].

In order to illustrate the Impairment Threshold concept in translucent optical networks, consider the topology example shown in Figure 1 with IT=2, which means that a route in this network will be considered feasible only if after 2 hops there is a node to regenerate the optical signal quality (regenerator node). For instance, consider the two routes (Figure 1) between a generic source-destination pair: route A and route B. Observe that while route A shows to be unfeasible because it has four hops without regeneration, on the other hand, route B appears to be feasible because after 2 hops the optical signals are regenerated (in R), reaching destination with two more hops.

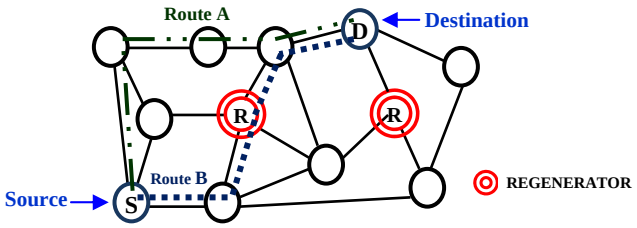


Figure 1. Example of routing in a translucent optical network.

The rest of this article is organized as follows. In Section II, previous related works are discussed. Section III introduces the shortest path selection problem for translucent optical networks. Section IV presents the new routing heuristic proposed, which performance is evaluated in Section V. Final remarks are made in Section VI.

II. RELATED WORKS

The optical signal impairment-aware routing and the wavelength assignment problems have been recently studied by many researchers [2,8,10,11,12].

In [10], one can find a survey about optical-physical-layer-aware RWA algorithms where different strategies are classified as single path or multi-path. Multi-path or multiple routes strategies search any feasible route out of *n* routes to satisfy a lightpath request. All those strategies use the shortest path algorithm for route calculation.

Rai et al. [12] proposed an information search-based algorithm for translucent optical networks that chooses feasible routes with minimal hops.

The Polynomial time Impairment Aware Routing Algorithm (PIARA) for translucent optical networks with sparse placement of regenerators is proposed in [8]. PIARA computes link costs based on optical physical impairments, and searches for feasible shortest routes passing, if necessary, through regenerator nodes. Feasible routes are obtained by means of a module based on a classical shortest path algorithm that does not use pre-computed routes. Therefore, PIARA can be considered as an exhaustive routing class algorithm.

All routing strategies used in those previous related works are based on shortest path algorithms (*e.g.*, Dijkstra`s algorithm [5]). Because they are based on or have a module implementing classical shortest path algorithms in their solutions, these routing strategies do not properly consider the case where there is more than one feasible shortest path to choose from.

In this work, we try to put in evidence this unique-best-shortest-path problem of the existing shortest path algorithms for translucent optical networks which are characterized by a reach limit for the optical signal propagation. Besides, we propose a new routing strategy for translucent optical networks, named BSTL, which main routing features are: adaptive, optical-physical-layer-impairment-aware, multiple-best-shortest-path-aware, and resource utilization efficiency.

 ISBN: 978-1-61208-231-8

III. THE PROBLEM OF CHOOSING THE BEST AMONG *M* COMBINATIONS OF FEASIBLE SHORTEST PATHS IN TRANSLUCENT OPTICAL NETOWRKS

Durães et al. [6], introduced the problem of choosing the best combination among *M* Combinations of Shortest Paths (MCSP) where multiple options of shortest paths for routing in transparent optical networks result in different performance issues. In this section, the MCSP problem is extended to the case of translucent optical networks.

In translucent optical networks some paths are considered unfeasible routes due to optical physical layer impairments. Therefore, only shortest paths which are feasible routes will be taken into account hereafter.

Considering an optical network topology with *N* nodes, the total number of source-destination pairs is $N \times (N-1)$. We will use the notation *pair(s,d)* to represent an ordered pair of nodes, with its origin at node *s* and its destination at node *d*. For adaptive routing, it is necessary to set a dynamic route for each path request. If we assume that the *pair(s,d)* uses the same route as the *pair(d,s)* (bidirectional path), then it is sufficient to find forward routes only. Therefore, at least $R = (N \times (N-1))/2$ routes have to be computed for a determined topology with *N* nodes, in order to satisfy any path request *(s,d)*.

Most of the related works (Section II) use classical shortest path algorithms (e.g., Dijkstra's and Bellman–Ford's) to compute routes or to compose a routing solution, fixed, alternate or exhaustive. These classical algorithms, which usually are implemented as "modules" in others algorithms, aim at finding one shortest path for each *pair(s,d)*. However, between any two nodes (source and destination) it may be found more than one shortest paths. To illustrate this, consider a simple example of a translucent optical network based on the topology shown in Figure 2, here named as **R**ing with **6** **N**odes and one **T**ransversal **L**ink (R6NTL), where node 2 is a regenerator node. For instance, we observe that there are two shortest feasible paths between nodes 1 and 4 in R6NTL, either with three hops: 1–2–3–4 and 1–2–5–4. Therefore, without any other additional criterion, a classical shortest path algorithm applied to R6NTL may choose any of these three-hop paths for routing between nodes 1 and 4.

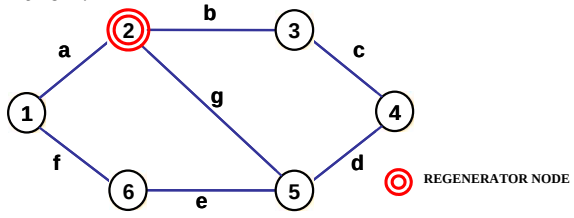


Figure 2. R6NTL Topology.

Now, generalizing to any translucent optical network topology, as for each *pair(s,d)* there may be more than one shortest path feasible route (called in this work Feasible Candidate Routes – FCR), there are *M* different solutions for selecting the feasible routes in a given network topology. The number *M* of possible solutions is given by

$$M = \prod_{i=1,\, j=1}^{N,N} FCR_{pair(i,j)} \qquad (1)$$

where $FCR_{pair(i,j)}$ represents the number of shortest path feasible candidate routes for the *pair(i, j)*, with $i \neq j$. Note that all candidate feasible routes have the least number of hops.

For the R6NTL topology, we have $M = 1^9 \cdot 2^6 = 64$ because this topology has nine pairs of source–destination nodes with only one feasible candidate route and six pairs with two shortest path feasible candidates. So, considering all shortest path feasible candidate routes for each *pair(s,d)* in the R6NTL topology, there are M = 64 different combinations of feasible shortest paths.

Table 1 shows all shortest path feasible candidate routes for each *pair(s,d)* in the R6NTL topology. For later comparison purpose, the routes computed by the PIARA algorithm [8] are indicated by an asterisk in Table 1.

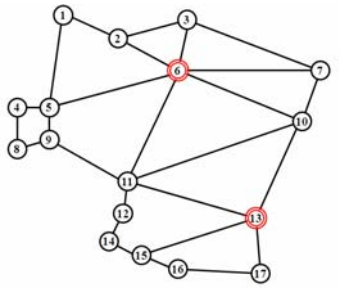
TABLE I. FEASIBLE SHORTEST PATHS FOR R6NTL TOPOLOGY.

Pair (*s,d*)	**Feasible Shortest Path**	**Pair (s,d)**	**Feasible Shortest Path**
(1,2)	1-2*	(2,6)	2-1-6* 2-5-6
(1,3)	1-2-3*	(3,4)	3-4*
(1,4)	1-2-3-4* 1-2-5-4	(3,5)	3-2-5* 3-4-5
(1,5)	1-2-5*	(3,6)	3-2-1-6* 3-2-5-6
(1,6)	1-6-5*	(4,5)	4-5*
(2,3)	2-3*	(4,6)	4-5-6*
(2,4)	2-3-4* 2-5-4	(5,6)	5-6*
(2,5)	2-5*		

We can then define the problem of choosing the best combination among *M* Combinations of Feasible Shortest Paths (MCFSP) as how to identify a solution of feasible shortest paths routes S_k with $1 \leq k \leq M$, such that S_k provides the best network blocking probability performance. This new definition generalizes for translucent optical networks the previous definition of the MCSP problem [6].

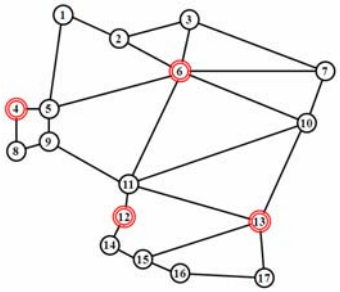
To illustrate the MCFSP problem we can consider, besides R6NTL, the Germany and the European Optical Network (EON) topologies shown in Figure 3, two interesting topologies for translucent optical network studies [8,12], all having regenerator nodes placed randomly in such a way that there are no two adjacent nodes with regeneration capability. Table 2 presents the number of routes R of a solution S_k, the sum of the number of feasible candidate routes (ΣFCR) for all *pairs(s,d)* and the number *M* of solutions of the MCFSP problem considering different scenarios in terms of topology, regenerator placement and optical reach (i.e., Impairment Threshold).

 ISBN: 978-1-61208-231-8



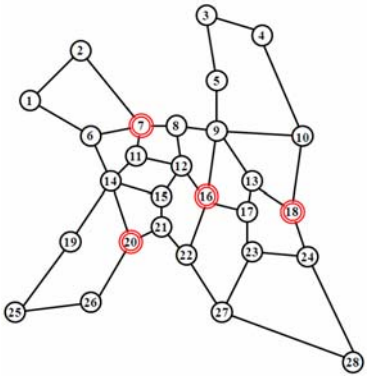
OEO NODE

a) Germany Topology with 2 OEO nodes



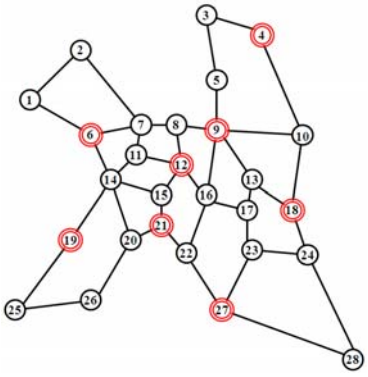
OEO NODE

b) Germany Topology with 4 OEO nodes



OEO NODE

c) EON Topology with 4OEO nodes



OEO NODE

d) EON Topology with 8 OEO nodes

Figure 3. Examples of translucent optical network topologies [12].

TABLE II. EXAMPLES OF THE MCFSP PROBLEM.

Network Topology	R	OEO Nodes	Optical Reach (*IT*)	ΣFCR	*M*
R6NTL (Fig. 2)	15	1	2 Hops	21	64
Germany Topology (Fig. 3)	136	2	2 Hops	368	$5{,}19 \times 10^{33}$
			3 Hops	472	$1{,}35 \times 10^{48}$
			5 Hops	526	$3{,}76 \times 10^{57}$
		4	2 Hops	398	$3{,}02 \times 10^{35}$
			3 Hops	480	$2{,}16 \times 10^{49}$
			5 Hops	526	$3{,}76 \times 10^{57}$
EON Topology (Fig. 3)	378	4	2 Hops	432	$3{,}02 \times 10^{23}$
			3 Hops	1074	$1{,}92 \times 10^{100}$
			5 Hops	1588	$7{,}43 \times 10^{68}$
		8	2 Hops	765	$1{,}18 \times 10^{169}$
			3 Hops	1620	$6{,}20 \times 10^{71}$
			5 Hops	1800	$1{,}04 \times 10^{189}$

In Table 2, we observe that the value of *M* increases very fast with the number of node pairs (*R*) and the number of feasible candidate routes for a specific *pair(s,d)*. Furthermore, we observe that the decrease of the optical reach (IT) reduces the number of feasible candidate routes too. However, even under low IT values (e.g., 2), the number of feasible shortest path combinations remains very high. This appears to be a good opportunity to apply new criteria to select feasible shortest paths in an adaptive routing scenario.

Algorithms using modules based on classical shortest path algorithm can find any solution S_k from the *M* solution set of the MCFSP problem. This happens because they do not consider any additional criterion in order to identify the best among the *M* possible solution combinations.

In order to show the variability of the network performance in terms of blocking probability when choosing from *M* combinations of shortest paths, we simulated all the $M = 64$ possible combinations of feasible shortest paths for R6NTL. In this case, it was found the best combination of feasible shortest path routes because of the simplicity of this topology, characterized by a few nodes and links. However, simulating all feasible shortest path combinations becomes impracticable with larger topologies (Figure 3 and Table 2).

Figure 4 shows a graph with 64 blocking probability curves for a hypothetical translucent optical network with the topology R6NTL (IT=2) as shown in Figure 2. The characteristics of this simulation study (number of lightpath requests generated, traffic type, wavelength assignment algorithm, etc.) are the same described later in Section V.

 ISBN: 978-1-61208-231-8

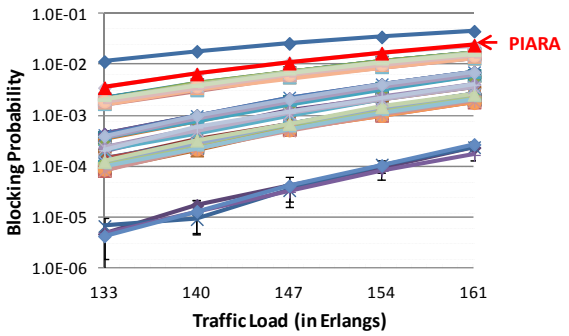


Figure 4. Blocking probability of all feasible shortest route combinations (M=64) of the R6NTL/IT=2 scenario.

Each curve in Figure 4 represents the performance in terms of blocking probability of one routing solution among the M = 64 possible solutions of the MCFSP problem as a function of the traffic load. The routing solution found by the PIARA algorithm [8] (Table 1) is highlighted for comparison purposes. Notice that PIARA, even being an exhaustive routing algorithm, will always find the same routes, as long as the optical reach (i.e., IT) remains the same. On the other side, these results (Figure 4) clearly show the large variability of performance among the several possible routing solutions, justifying a judicious planning strategy for choosing the set of feasible shortest routes in a translucent optical network.

Note that the number of combinations M in Table 2 is computed using Equation 1. A modified Dijkstra's algorithm is used only to compute the shortest path feasible routes (FCR) for each pair. The performance evaluation using all feasible route combinations in a small network (R6NTL) intends to exemplify the diversity of solutions of the MCSP problem, not to solve it. Actually, in larger networks, the routing strategy must avoid the need of scanning all feasible route combinations.

IV. PROPOSED HEURISTIC

This section presents a new algorithm for translucent optical networks named Best Shortest Translucent Lightpath (BSTL), which is an optical physical layer impairment-aware and adaptive routing algorithm. BSTL uses the link utilization measure (number of used wavelengths) to find the best solution for the MCFSP problem. The goal of BSTL is to balance the load among all links while reducing the blocking probability of lightpath requests, without breaking the optical physical layer constraints.

The execution of BSTL, as for any adaptive routing algorithm, is divided into two steps: alternate route computation and operation. The alternate route computation step occurs in the network planning phase. At the first step, all shortest routes for each *pair*(*s*,*d*) are previously computed by a modified Dijkstra's algorithm and stored for later checking and selection. For instance, for the R6NTL, the pre-computed BSTL routes are shown in Table 1. The second step of BSTL execution coincides with the operational phase where BSTL chooses, among the pre-computed set of feasible shortest paths, the feasible route with more availability of free continuous wavelengths to satisfy a specific source-destination lightpath request. This dynamic routing characteristic of BSTL is inspired in the Least Loaded Routing (LLR) algorithm [13]. LLR tries to satisfy a lightpath request using always the first of an ordered set of pre-computed alternative routes. Only if the first pre-computed route has no available resources, LLR will sequentially search a route among the other pre-computed alternative routes. However, as opposed to LLR, BSTL has a compromise with load balancing (frequency of use of wavelengths) among all pre-computed alternative routes.

A summary of the BSTL steps is as follows:

1) [Planning Phase] – Compute all shortest routes for each *pair(s,d)* by a modified Dijkstra's algorithm;
2) [Operational Phase] – Returns the feasible route, among the pre-computed ones, which has more available free continuous wavelengths.

The main idea of the BSTL is, at first, to compute off-line all feasible routes for each *pair(s,d)*, which is different from computing and simulating all M combinations of route solutions for a given topology and, secondly, to use the continuous wavelength availability criterion to dynamically select routes among the feasible routes pre-computed in a *pair(s,d)* basis. The load balancing strategy adopted by BSTL acts in order to prevent link bottlenecks which trends to compromise the network overall performance.

V. PERFORMANCE EVALUATION

The performance of BSTL was evaluated at different scenarios and compared to PIARA [8]. The different topologies and regenerator placements (randomly distributed, avoiding neighbor nodes) studied were those shown in Figures 2 and 3. The main metrics considered were network utilization and blocking probability. An additional metric corresponding to the fairness in satisfying the lightpath requests was also evaluated. The simulation tool TONetS [14] was extended to support the new characteristics of the translucent network routing algorithms here studied.

This simulation study, as well as the simulation results previously presented (Section III), has the following basic characteristics, usually assumed in similar studies about circuit-switched optical networks. Traffic demand is characterized by optical circuit (i.e., lightpath) requests in a *pair(s,d)* basis, uniformly distributed among all $N \times (N-1)$ pairs. Requests are generated based on a Poisson process with average rate λ and the lightpaths' hold times are exponentially distributed with mean $1/\mu$. The network's traffic intensity in Erlangs is given by $\rho=\lambda/\mu$. All network's links are bidirectional, having 40 wavelengths for each direction. *First-Fit* [4], by simplicity and good performance reasons, is used as the wavelength assignment algorithm. For each simulation, five replications are performed and five millions requests are generated for each replication. All graphical results express confidence intervals evaluated at the 95% confidence level.

 ISBN: 978-1-61208-231-8

A preliminary comparison between BSTL and PIARA, considering the R6NTL topology (Figure 2), is presented in Figure 5. The average utilization per link using BSTL or PIARA (under 161 Erlangs) is shown in Figure 5a. With PIARA, links ‘‘a” and ‘‘b” appear to be *overloaded* with an average utilization of 77%, approximately, while links ‘‘d” and ‘‘e” may be considered *underloaded* with an average utilization equal to 26%, approximately. On the other side, with BSTL, the average utilization of every link remains between 38% and 56% (Figure 5a), showing its effectiveness in terms of load balancing among the network’s links. Figure 5b shows the performance of BSTL and PIARA in terms of blocking probabilities. Observe that with BSTL, the route chosen for a specific lightpath request for the *pair(s,d)* cannot be the same route that satisfied the last request for the same pair. For instance, the BSTL solutions as shown in Figure 5b achieved a blocking probability performance of 0.0005, approximately, at the last load point (161 Erlangs), while PIARA achieved 0.024 under the same load.

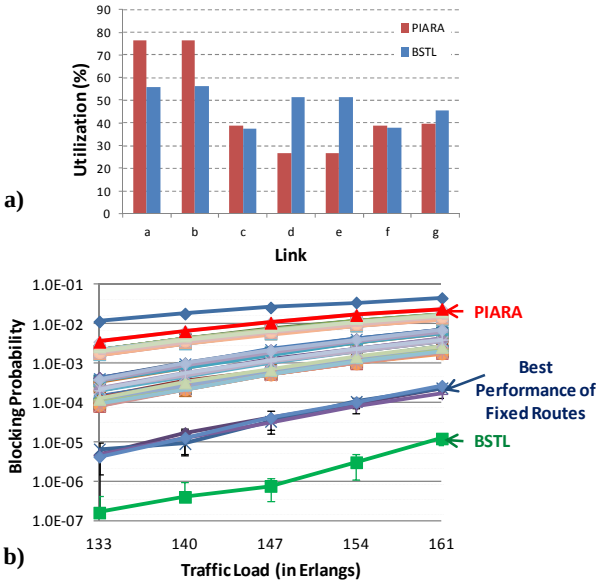


Figure 5. Link Utilizations (a) and Blocking Probabilities (b) for BSTL and PIARA algorithms in the scenario R6NTL/IT=2.

The average run time of PIARA in this preliminary study, considering the R6NTL/IT=2 scenario, was 1.1 millisecond, while BSTL took 0.04 millisecond for the same scenario. Notice that PIARA does not compute any route previously. On the contrary, PIARA computes routes dynamically under requests and considering the present state of the network. Therefore, as PIARA can select among any possible route, it would be expected its superior performance when compared to an alternate algorithm like BSTL which select routes from a pre-computed list. However, PIARA has a more complex implementation than BSTL, justifying its inferior run time behavior. With PIARA, it is necessary to gather link state information from all network links to compute partial routes and to generate the auxiliary graph that will conduct the selection of the final route. The BSTL strategy has an implementation less complex in the operational phase, because only links that compose the set of feasible candidate routes (pre-computed) are analyzed in the route selection procedure.

BSTL is also compared to PIARA considering the different topologies and OEO node placements shown in Figure 3. Firstly, the comparison is carried out in terms of blocking probabilities and network utilizations (Subsection A). Afterwards, fairness for each *pair(s,d)* is evaluated (Subsection B).

A. *Blocking probabilities and network utilizations*

The performance evaluation results with BSTL and PIARA in terms of blocking probabilities and network utilizations (i.e., average of the utilization of each network link) are presented in Figures 6.a to 6.d, considering the topologies of Figures 3a to 3d, respectively. The results achieved show a superior performance of BSTL for all evaluated scenarios. The better performance of BSTL can be explained because the routes chosen for each *pair*(*s,d*) are one of a *M* shortest path combination, and additionally, they are chosen aiming at link load balancing. On the other side, PIARA does not employ any additional criterion to choose a route besides the shortest path one.

From the network utilization point of view (Figure 6), BSTL's performance also appears to be superior because its lower blocking of lightpath requests; it also makes clear the advantages of its load balancing strategy. PIARA, which does not have a load balancing issue, becomes vulnerable to some “bottleneck links”, resulting in higher blocking probabilities and lower network utilizations than with BSTL.

B. *Fairness*

The metric of (average) blocking probability shows a general view of the success probability of satisfying a lightpath request in a specific topology scenario. Despite its usefulness, an average blocking probability metric tends to conceal the variability of blocking probabilities experimented by each *pair(s,d).* In order to evaluate the impact of blocking probabilities in a *pair(s,d)* basis we define the fairness in satisfying a lightpath request as follows [15]:

$$Fairness = \frac{1 - Max\left(B_{p(s,d)}\right)}{1 - Min\left(B_{p(s,d)}\right)} \qquad (2)$$

where Bp(s,d) is the blocking probability for the pair(s,d).

This formula computes the ratio between the average blocking probability of the *pair(s,d)* with the worst performance and the blocking probability of the *pair(s,d)* with the best performance. The graphs presented in Figure 7 show BSTL's and PIARA's performances in terms of fairness for the topologies in Figure 3. It can be observed from these graphs that BSTL achieves better performances than PIARA for all evaluated scenarios. These superior performance results can also be explained by BSTL's load balancing strategy.

 ISBN: 978-1-61208-231-8

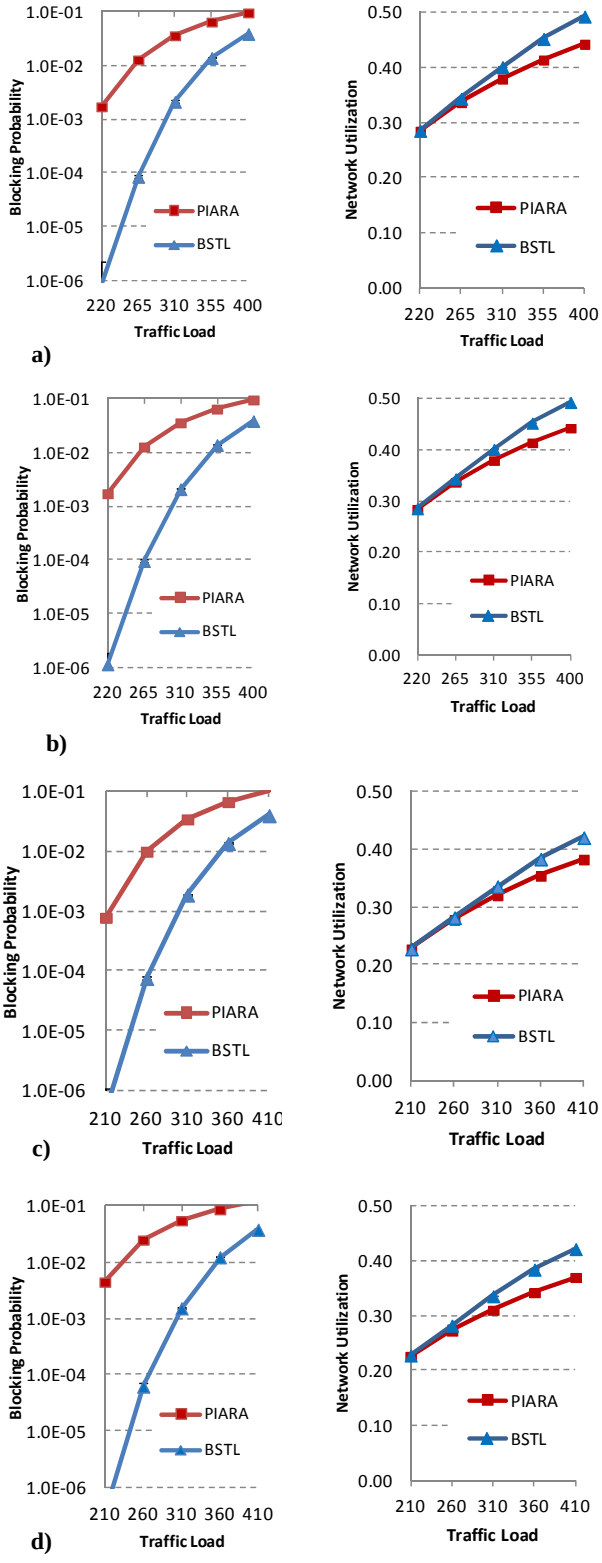


Figure 6. BSTL's and PIARA's blocking probability and network utilization performances.

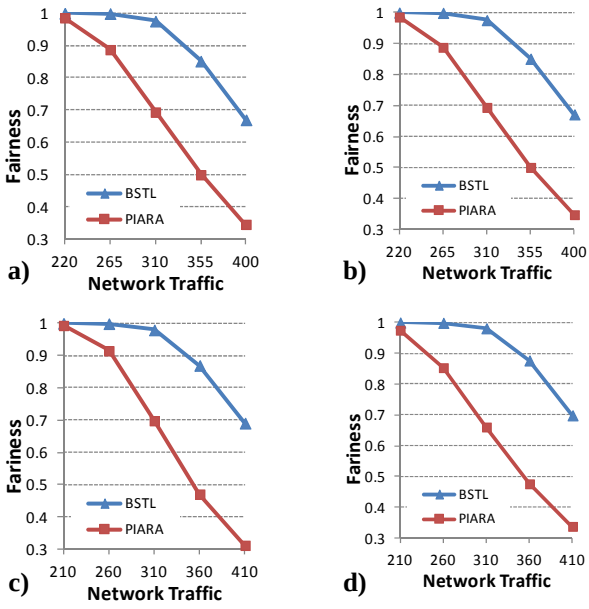


Figure 7. BSTL's and PIARA's fairness performances.

We also carried out performance studies of BSTL and PIARA with others topologies as the ones presented in [8] and [12]. In all the cases studied, BSTL achieved better performances.

VI. FINAL REMARKS

This work presented a reformulation of the problem of the best choice of the shortest paths for translucent optical networks and proposed a new adaptive routing algorithm, named Best Shortest Translucent Lightpath (BSTL), that simultaneously considers optical physical layer constraints, shortest paths, and dynamic load balancing objectives. This new routing strategy had its performance evaluated and compared to another algorithm previously proposed in the literature, showing its superior performance in terms of network utilization, blocking probability and fairness when applied to translucent optical networks.

REFERENCES

[1] M. J. O'Mahony, D. Klonidis, and D. Simeonidou, "Future Optical Networks", *Journal of Lightwave Technology*, 24:4684-4696, 2006.

[2] M. Gagnaire, and S. Zahr. "Impairment-Aware Routing and Wavelength Assignment in Translucent Optical Networks: State of the Art". *IEEE Comm. Mag.*, 47(5):55-61, May, 2009.

[3] G. Shen and R. S. Tucker. "Translucent Optical Networks: The Way Forward". *IEEE Comm. Mag.*, 45(2), Feb., 2007.

[4] H. C. Lin, S. W. Wang, and C. Tsai, "Traffic Intensity Based Fixed-Alternate Routing in All-Optical WDM Networks", *in Proceedings of the IEEE ICC*'2006, Istanbul, Turkey, June, pages 11 – 15, 2006.

[5] E. W. Dijkstra, "A Note on Two Problems in Connection with Graphs", *Numerical Mathematics*, 1:269–271, 1959.

[6] G. M. Durães, A. C. B. Soares, J. R. Amazonas, and W. F. Giozza, "The choice of the best among the shortest routes in transparent optical networks", *Computer Networks*, 54:2400-2409, 2010.

[7] P. Rajalakshmi and A. Jhunjhunwala, "Load Balanced Routing to Enhance the Performance of Optical Backbone Networks", *in 5th*

IFIP Int. Conf. on Wireless and Optical Communications Networks (WOCN 2008), Surabaya, Indonesya, 2008.

[8] F. Kuipers, A. Beshir, A. Orda, and P. Van Mieghem, "Impairment-aware Path Selection and Regenerator Placement in Translucent Optical Networks," *Proc. of the 18th IEEE International Conference on Network Protocols (ICNP 2010)*, Kyoto, Japan, October, 5-8, 2010.

[9] K. Manousakis, P. Kokkinos, K. Christodoulopoulos, and E. Varvarigos. "Joint Online Routing, Wavelength Assignment and Regenerator Allocation in Translucent Optical Networks", *Journal of Lightwave Technology*, 28(8):1152-1163, April, 15, 2010.

[10] S. Azodolmolky, M. Klinkowski, E. Marin, D. Careglio, J. S. Pareta, and I. Tomkos, "A survey on physical layer impairments aware routing and wavelength assignment algorithms in optical networks", *Computer Networks*, 53:926-944, 2009.

[11] J. Strand and A. Chiu, "Impairments and Other Constraints on Optical Layer Routing," *RFC 4054*, May, 2005.

[12] S. Rai, C-F Su, and B. Mukherjee, "On provisioning in all-optical networks: an impairment-aware approach", *In: IEEE/ACM Transactions on Networking*, 17(6):1989-2001, 2009.

[13] A. Birman, "Computing Approximate Blocking Probabilities for a Class of All-optical Networks," *IEEE Journal on Selected Areas in Communications*, 14(5):852-857, June 1996.

[14] A. C. B. Soares, G. M. Durães, W. F. Giozza, and P. R. F. Cunha, "TONetS: Transparent Optical Network Simulator" *in VII Tools Demos of the 26th Brazilian Computer Networks and Distributed Systems Symposium, (SBRC 2008)*, Rio de Janeiro, Brazil, 26-30 May 2008 *(available in Portuguese*).

[15] A. C. B. Soares, W. F. Giozza and P. R. F. Cunha, "Classification Strategy to Mitigate Unfairness in All-Optical Networks", *in 15th IEEE International Conference on Networks (ICON)*, Adelaide, Australia, 19-21 November, 2007.

 ISBN: 978-1-61208-231-8

Performance Analysis of Hybrid Optical Networks (OCS/OBS) considering the Time Period to Successfully Deliver a Data Flow

Felipe Mazullo, Igo Moura, André Soares
Federal University of Piauí - UFPI
Distributed Systems and Computer Networks Laboratory
Teresina, Brazil
e-mail: felipe.mazullo@ufpi.edu.br,
igo.moura@ufpi.edu.br, andre.soares@ufpi.edu.br

José Maranhão
University of Campinas - UNICAMP
Campinas, Brazil
e-mail: j3maranhao@gmail.com

***Abstract*— This paper presents a performance evaluation study that compares Optical Circuit Switching (OCS), Optical Burst Switching (OBS) and OCS/OBS networks. This study considers two types of traffic flow, long (5GB) and short (50MB). The main contribution of this paper is comparing such switching paradigms in terms of the time to successfully deliver a flow. Besides, we identify the problem of blocking due to outdated information when OCS network works under short data flow.**

Keywords-All-Optical Networks; WDM; Simulation Tool.

I. INTRODUCTION

The popularity of the Internet and the emergence of sophisticated applications are demanding more bandwidth in transport network links [1]. Figure 1 shows the average annual growth rate of international Internet traffic between 2007 and 2011. In 2010-2011, for example, the average Internet traffic growth was 47%. Applications involving voice, video-on-demand, teleconferencing, high-resolution medical imaging and e-science applications have increased the bandwidth demands in transport networks. In general, these sophisticated applications need to transfer large volumes of data under high Quality of Service (QoS) requirements.

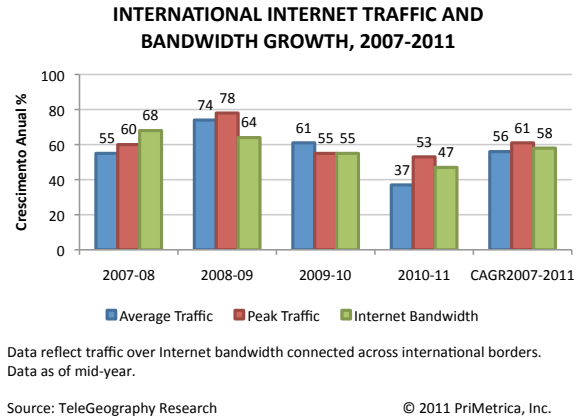


Figure 1. Average annual growth of international Internet traffic between 2007 and 2011. Adapted from [2]

A new generation of networks is based on an optical infrastructure that has been developed to support the growth of Internet traffic. This infrastructure uses optical fibres, which are mainly characterised by their ability to provide high bandwidth and their immunity to noise and electromagnetic interference. The use of this new material is justified by the existing infrastructures incapacity to efficiently serve a growing number of users and sophisticated applications. The use of Wavelength Division Multiplexing (WDM) can increase the efficient use of bandwidth in optical fibres [3]. With WDM technology, it is possible to establish multiple optical channels working at different wavelengths simultaneously in a single optical fibre.

WDM optical networks can be classified as opaque or transparent. In a transparent optical network, intermediate nodes transmit signals without converting them to electronic impulses. Opaque optical networks perform wavelength routing in the electronic domain. Therefore, each network node must convert the optical signal into an electrical signal and vice versa. Opto-Electro-Optical (OEO) converters are needed to convert the signal. The disadvantage of OEO converters is that they introduce processing delays. In transparent optical networks, wavelength routing is performed in the optical domain and does not require OEO converters, eliminating this limitation [3].

In general, the available methods for data switching in transparent optical networks are: Optical Circuit Switching (OCS), Optical Packet Switching (OPS) and Optical Burst Switching (OBS). In addition, there are hybrid architectures that combine these existing paradigms.

To transfer information in transparent optical networks, it is necessary to define a route and to assign a wavelength to each route's link. This is known as the Routing and Wavelength Assignment (RWA) problem. RWA algorithms aim to simultaneously minimise the blocking probabilities of circuits, bursts and packets [4], [5].

This paper presents a performance evaluation study of OBS, OCS and hybrid OBS/OCS network. The main contribution of this paper is comparing such switching paradigms in terms of the time to successfully deliver a flow. Besides, we identify the problem of blocking due to outdated information when OCS network works under short data flow. The remainder of this paper is organised as follows. A description of switching paradigms is presented in Section II. The TONetS simulator is

 ISBN: 978-1-61208-231-8

presented in Section III. How the switching paradigms function is discussed in detail in Section IV. Section V reviews relevant literature. Sections VI and VII present our results and conclusions, respectively.

II. SWITCHING PARADIGMS

The most important feature of the OCS paradigm is the reservation of resources (wavelengths) in the establishment phase of the optical circuit (lightpath) [5]. The source node sends a control message before sending the data. This message aims to reserve the necessary bandwidth and configure the optical cross-connect (OXC) along the data's route. The data are sent only after the source node receives a confirmation message that bandwidth has been reserved. OCS systems allow resource reservation with high QoS, but they are not very efficient for short communications.

The OPS paradigm is the least developed of the three switching strategies [6]. OPS is a more efficient alternative when traffic is characterised by a high rate of change in the presence of data packets of variable lengths. OPS switching does not use resource reservation, making it difficult to guarantee QoS in this paradigm. Due to limited progress in processing and optical storage, we consider this technology insufficiently mature.

The OBS paradigm uses optical bursts. A burst is a set of data packets sent to the same destination [7]. In an OBS system, a control message is sent before the burst to try to reserve the necessary bandwidth and configure the OXCs along the route. However, OBS does not wait for a message to confirm the reservation of resources. The optical burst is sent without a guarantee of successful resource allocation.

The literature addresses OBS as a flexible alternative suitable for transporting small volumes of traffic through a transparent optical network [7], [8]. This alternative is more appropriate for scenarios that require less rigorous QoS. By using bursts, it is possible that a given data flow will exceed the maximum size of the burst. When this occurs, the flow is fragmented and sent in several separate bursts. This requires a control message for each burst, and may cause signalling overhead.

Hybrid optical switching (OCS/OBS) is an alternative switching paradigm that allows OCS or OBS in the same network infrastructure. Previous research has addressed the mechanism required to decide which switching strategy should be used to serve a given request in this type of switching architecture [9], [10]. In a scenario with several different classes of users, a service provider should be able to offer differentiated services. That is, a WAN service provider must have the ability to provide services with higher or lower levels of QoS that approximate actual demand.

Under heterogeneous scenarios, OBS is thought to be a good alternative for short-term network services, while OCS should be used for long-term network services. In this scenario, given the different characteristics of circuit switching and burst switching, a hybrid OCS/OBS network should be the optimal solution for a diverse set of users. Users with high QoS requirements can use the dynamic provisioning of circuits, while users who demand small volumes of data can use the OBS switching service.

This work focuses on a hybrid network that allows circuit switching or burst switching within the same network. Our study simulates the performance of a hybrid OCS/OBS switching architecture.

III. TONETS

The TONetS (Transparent Optical Network Simulator) simulation tool is a discrete event simulator developed in the Java programming language. TONetS was integrated with OB2S [8]. Both simulators were developed for specific switching technologies. The former simulates OCS networks, and the latter simulates OBS networks. We used the following metrics present in TONetS to assess performance:

- Blocking probability: the probability that a given request arriving in the optical network is blocked.
- Blocking probability due to outdated information: also called backward blocking [11]; the blocking of a request due to outdated network state information. This occurs when a request notes that a wavelength is free, but in the time required to perform the allocation, the resource is assigned to another request.
- Queue time: the time that a request spends in the queue of blocked requests waiting to be sent.
- Signalling time: the time spent on signalling messages in the control plan before actual data transmission.
- Successful delivery time: the time between the arrival of a data flow in the optical network and the instant that flow is transferred successfully. This time is the sum of the Queue Time, Signalling Time and Transmission Time.

IV. SWITCHING PARADIGMS PRESENT IN THE SIMULATOR

A. OCS

To establish a connection between two nodes in an OCS network, the required resources (wavelengths) must be reserved for the selected route. Signalling messages are sent through the control plane to reserve these wavelengths. Each node in the route processes these messages. Figure 2 shows the OCS control plane procedures.

 ISBN: 978-1-61208-231-8

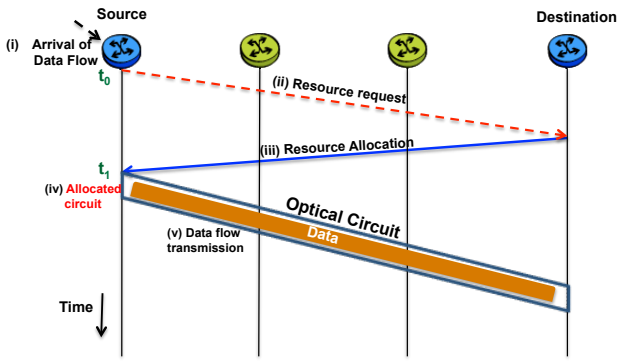


Figure 2. OCS Control Plane

With the arrival of a circuit request, the source node sends a control message requesting the reservation of resources. Each node in the route receives this message, processes it, and forwards the control message requesting resources to the next node in the route. When the message reaches the destination node, this node runs the wavelength algorithm, sets up its OXC, allocates the wavelength in its link, and then sends back a reserve message to the other nodes in the route, in reverse order. In the backward direction, each node receives the message, processes the message, sets up its OXC, allocates one wavelength and sends the message to the preceding node. This process is repeated until the source node receives the reserve message and configures its OXC. After this establishment process, the circuit is ready to transfer the data flow.

B. OBS

In an OBS, the source node first assembles the burst. The burst contains packets that arrive at a given source node of the OBS network. These packets come from access networks (i.e., the client networks of an OBS network). One burst can only contain packets with the same destination node. In addition to building bursts, the edge node must be able to disassemble bursts. The data from the disassembled bursts are forwarded to access networks across the optical network.

The OBS that we implemented in TONetS takes into account two signaling protocols, JIT (Just in Time) and JET (Just Enough Time) [12]. A signalling protocol defines how message exchanges are made and when the allocation and release of resources occurs. In this simulation, the JIT signaling protocol is used for OBS switching. It uses explicit allocation and implicit resource releasing (i.e., a node does not have to wait for a control message to know when to release a resource). The node itself can predict when to release the resources because the control message contains the size of the burst to be sent.

In OBS, a peculiarity occurs when the data flow that will be sent exceeds the maximum size of the burst. In this case, the data flow must be fragmented into several bursts, which are sent individually. However, in OCS the data flow is not fragmented. In our OBS model, the data flow is fragmented, and its packets are mounted in several bursts. Therefore, a signaling message is required in the OBS, as shown in Figure 3.

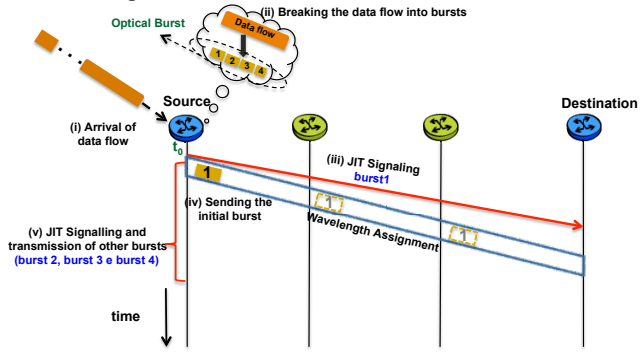


Figure 3. The fragmentation of a data flow into burst

C. Hybrid OCS/OBS Network

The hybrid network implemented in our simulation is similar to the parallel architecture presented in [13]. The edge node of the network classifies the data flow as long or short. Long flows are sent using the OCS paradigm, and short flows are handled by the OBS paradigm. However, in our parallel architecture model, the OBS and OCS paradigms share resources, aiming for better network utilisation.

V. RELATED WORKS

Several studies have been carried out comparing the performance of OCS and OBS paradigms without a hybrid model [14], [15], [16], [17], [18].

J.P. Jue and V.M. Vokkarane [14] evaluated these two switching paradigms taking into account three metrics: the blocking probability, the throughput and the recurrent blocking probability of a given request (circuit or burst), i.e., the probability that a request is blocked more than once.

A. Zalesky [15] proposed an analytical model to study a queuing scenario. After analysing OCS and OBS paradigms with regard to blocking probability, queue delay and network utilization, the authors concluded that future transparent optical networks must use hybrid approaches to achieve a better utilisation of network resources.

The study presented in [16] performed a network utilisation analysis comparing an OCS network with three different approaches to OBS networks: a pure OBS strategy, OBS considering wavelength conversion and a last variation that considers both load balancing and wavelength conversion. The authors concluded that more research was needed to determine the appropriate paradigm for a variety of traffic conditions and available network resources.

Liu Xin, Qiao Chunming, Yu Xiang and Weibo Gong [17] investigated the rates of packet delivery and packet loss of OCS and OBS paradigms. In [18], the authors compared the financial costs of the OBS and OCS

 ISBN: 978-1-61208-231-8

networks equipment needs. The comparisons took into account the cost-effectiveness of these networks.

With regard to hybrid optical networks, C.M. Gauger, P.J. Kuhn, E.V. Breusegem, M. Pickavet and P. Demeester [13] proposed a classification, dividing hybrid networks into three types: client-server, parallel and integrated. The authors presented a client-server architecture and an integrated architecture. In [9] and [19], the authors presented parallel hybrid architectures.

Yeshuang Wang and Sheng Wang and Shizhong Xu and Xiufeng Wu [20] created a model for hybrid architecture and conducted a simulation of this architecture type. Compared with the OCS paradigm, the proposed hybrid model had the worst performance in regard to the time for a successful delivery. P.S. Khodashenas, J. Perelló, S. Spadaro, J. Comellas and G. Junyent [21] presented a different hybrid architecture, and a study of its financial cost and burst loss rate. We observed that the literature shows a deficiency of papers in which it is advantageous to use hybrid architecture.

Additionally, no studies were found that compared a hybrid paradigm to both the OCS and OBS paradigms regarding the successful delivery time of a data flow. It is noteworthy that this metric is relevant to the network user. Therefore, this paper presents a simulation comparing a hybrid architecture with the OCS and OBS paradigms regarding the time to successfully deliver the data flows.

VI. PERFORMANCE ANALYSIS

The experiments were carried out using the NSFnet topology, illustrated in Figure 4. Traffic is uniformly distributed between all source-destination node pairs. The request generation algorithm is a Poisson process with average rate λ, and the circuits' average hold time is exponentially distributed with the mean $1/\mu$. The network´s traffic intensity in Erlangs is given by $\rho = \lambda / \mu$. All links in the network are bi-directional and have 40 wavelengths in each direction. A randomisation algorithm is used for wavelength assignment. The maximum burst size is 250 MB.

For each simulation study in this article, 10 replications are performed with different, randomly generated, variable seeds, and 100,000 requests are generated for each replication. The graphical results present the confidence intervals evaluated at the 95% confidence level. Although confidence intervals have been plotted on all graphs in this article, they may be so small that they are hardly visible.

We assume a scenario with full wavelength conversion [4]. Therefore, it is not necessary for the assigned wavelength to be the same along the whole light path. We also considered the use of request queues. When a request is blocked (because no resources are available), the request is queued to be sent later when resources are available.

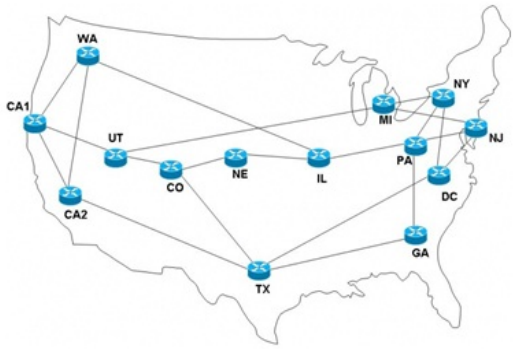


Figure 4. NSFnet Topology.

Figure 5.a shows the performance of OBS and OCS networks in terms of successful delivery time in a scenario with small data flows (50 MB). Figure 5.b shows the components of blocking probability (absence of resource and outdated information) when the network uses OCS technology.

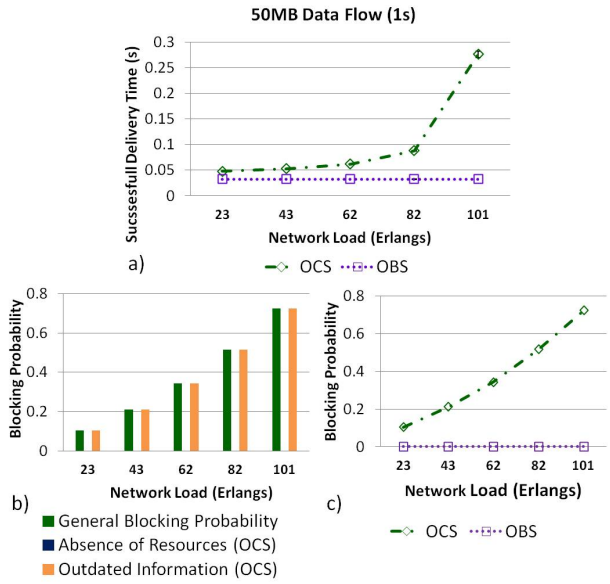


Figure 5. a) Time to successful deliver a flow of 50 MB. b) OCS Blocking Probability components of flows of 50 MB. c) OCS and OBS Blocking Probability under flows of 50 MB.

The OBS paradigm achieved better performance than the OCS paradigm when dealing with short data flows. The OBS paradigm delivery time also showed low growth as the network load increased compared to the OCS paradigm.

Of note in Figure 5.a is the worsening performance of OCS when the network load increases. In those cases, we incremented the request rate (λ) to increase network load ($\rho = \lambda / \mu$) because the average hold time must be proportional to 50 MB ($1/\mu = 0.01$ seconds). Therefore, when the request rate increases, the variability of the network resources also increases. This behaviour causes blocking due to outdated information in the network. The frequent changes in the state of the network promoted by

 ISBN: 978-1-61208-231-8

short data flow ends up generating a high probability of blocking due to outdated information concerning the state of the network. In fact, in these instances the network has available resources, but outdated information in the control plan causes blocking as shown in Figure 5.c. Blocked requests increase the average queue time, and consequently increase the successful delivery time.

Figure 6.a presents, for the same metric, the performance of OBS and OCS working with a long data stream (5GB). Figure 6.b depicts the blocking probability for each kind of switching paradigm (OBS and OCS) for the same scenario of Figure 6.a.

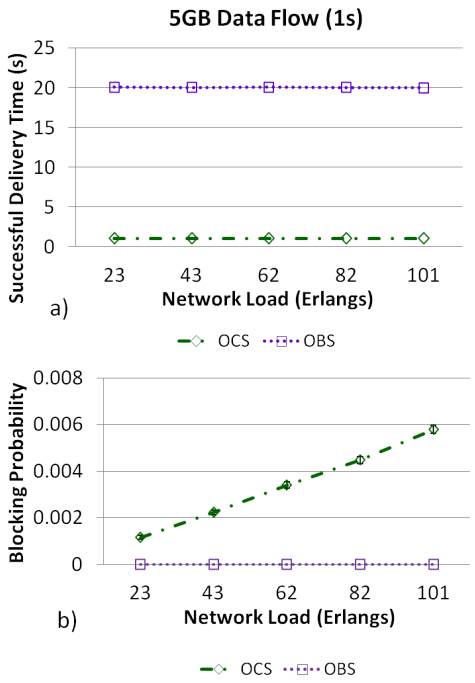


Figure 6. a) Time to successfully deliver a flow with an average duration of 1 second (5 GB). b) Blocking Probability in an OCS network.

For scenarios with an average flow under 5 GB, the OCS achieved better delivery time than the OBS paradigm. OBS must fragment the data when the flow is greater than the maximum burst size. For example, assuming the maximum size of the burst is equal to 250 MB, one flow of 5 GB must be fragmented into 20 bursts. As a result, one control message must be generated for each burst. Consequently, those control messages increase the overhead and the successful delivery time. For example, Figure 6.a shows that one flow of 1 second using OBS requires 20 seconds to be delivered successfully.

Although the OCS network presents a blocking probability worse than OBS (Fig. 6b), its performance in terms of time to successfully deliver a flow was better (Fig. 6a). In this situation, it is more relevant for the users the time to successfully deliver a flow. This behaviour showed that is important to study the time to successfully deliver a flow besides the blocking probability.

The frequency of state change in the network resources is very low under the traffic load considered, and with an average data flow of 5 GB. In this context, the blocking probability due to outdated control plan information is low, up to 100 times smaller than the blocking observed in Figure 5 scenario. Proportionally, the OCS paradigm performed better with data flows of 5 GB than with flows of 50 MB. In other words, the OCS paradigm performs better with long data flows. Previous studies indicate that the lower the duration of the circuit, the greater the likelihood of blocking due to outdated information [12].

Figure 7 illustrates the results for OCS, OBS and the hybrid (OCS/OBS) networks when subjected to two types of flow simultaneously. That is, when each node in the network generates 50% long flows and 50% short flows.

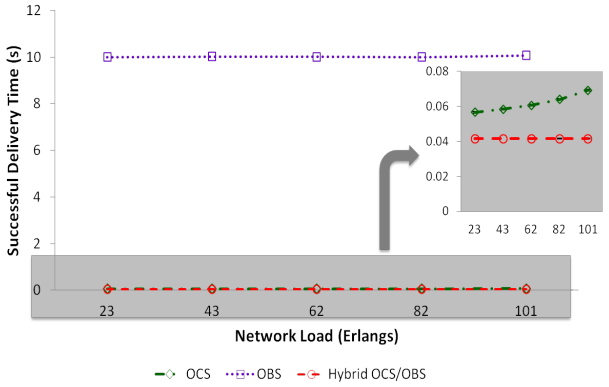


Figure 7. Successful delivery time in a OCS, OBS and Hybrid OCS/OBS network subjected to two types of flows.

The OCS network obtains a lower delivery time than OBS network. We believe that, in this scenario, the impact of signalling overhead in OBS was greater than the impact of blocking due to outdated information in OCS. For the hybrid network, we assume that the short flow is sent through OBS and the long flow is sent through OCS.

Figure 7 shows that the hybrid network delivery time is just above 0.04s. At first glance, this result might seem counter-intuitive given the fact that the OBS results in Figure 5.a are close to 0.04s while the OCS minimum time in Figure 6a is about 1 second. However, this occurs because the arrival rate of bursts is several times bigger than the arrival rate of circuits.

This simulation study increases the network load keeping the hold times (1/μ) equal to 0.01s and 1s for short and long flows, respectively. Besides, both flows generate the same network load. Therefore, the arrival rate of the OBS flow is 100 times bigger than OCS flows. The simulation results regarding the hybrid network delivery time can be verified by the following equation:

$$T = \frac{N_{OCS} * T_{OCS} + N_{OBS} * T_{OBS}}{N_{OCS} + N_{OBS}}$$

T is the hybrid paradigm delivery time, T_{OCS} is the OCS delivery time, $T_{OBS}$is the OBS delivery time and N_{OCS} and N_{OBS} are the OCS and OBS number of requests respectively. Replacing T_{OCS} for the value from Figure 6.a (1s), T_{OBS} for the value from Figure 5.a (aprox. 0.04s) and N_{OCS} and N_{OBS} for 1 and 100 respectively the resulting delivery time is similar to the results shown in Figure 7.

By weighting OCS and OBS delivery time in terms of their number of requests, the OBS delivery time had more impact the hybrid network delivery time which in turn presented a result just above 0.04 seconds.

The study showed that the hybrid (OCS/OBS) network obtained the best performance in terms of successful delivery time when compared with OCS and OBS networks.

VII. CONCLUSION

This paper presented a performance evaluation study, carried out via simulation that investigates the efficiency of a hybrid OCS/OBS paradigm. As shown in Section VI, our hybrid network presented a shorter successful delivery time than the traditional OBS and OCS paradigms.

The distinct behaviour of the OBS and OCS paradigms allows the hybrid OCS/OBS network to use the strengths of the two switching paradigms and enables it to succeed with a diverse set of users.

VIII. ACKNOWLEDGMENT

We would like to thank the *Fundação de Amparo a Pesquisa do Estado do Piauí* – FAPEPI and the Brazilian National Counsel of Technological and Scientific Development - CNPq for support of this work.

REFERENCES

[1] A. Szymaki, A. Lason, J. Rzasa, and A. Jajszczyk, Grade-of-service-based routing in optical networks", IEEE Communications Magazine, Feb. 2007, pp.82-87.

[2] Telegeography Research and Primetrica Inc. Executive Summary on Global Internet Geography. Free Resource Available in http://www.telegeography.com/research-services/global-internet-geography/index.html, retrieved: october, 2012.

[3] R. Ramaswami and K. N. Sivarajan, Optical Network - A Practical Perspective, 2rd ed., Morgan Kaufmann Publishers, 2002.

[4] H. Zang, J. P. Jue, and B. Mukherjee, A Review of Routing and Wavelength Assignment Approaches for Wavelength-Routed Optical WDM Network", SPIE Optical Networks Magazine, Jan, 2000.

[5] G. M. Durães, A. Soares, J. R. Amazonas, and W. Giozza, "The choice of the best among the shortest routes in transparent optical networks", Computer Networks, vol. 54, 2010, pp. 1389-1286, doi: 10.1016/j.comnet.2010.03.010.

[6] Y. Shun, B. Mukherjee, and S. Dixit, "Advances in photonic packet switching: an overview", IEEE Communications Magazine, vol. 38, Feb. 2000, pp. 84-94, doi: 10.1109/35.819900.

[7] C. Qiao and M. Yoo, "Optical Burst Switching (OBS) - a new paradigm for an optical Internet", Journal of High Speed Networks, vol. 8, Jan. 1999, pp. 69-84.

[8] J. Maranhao, H. Waldman, A. Soares, and W. Giozza, "Wavelength conversion architectures in OBS networks ", IEEE Network Operations and Management Symposium-NOMS, Apr. 2008, pp. 939 -942.

[9] Xin Chunsheng, Qiao Chunming, Ye Yinghua, and D. Sudhir, "A Hybrid Optical Switching Approach ", IEEE Global Telecommunications Conference-GLOBECOM, vol. 7, Dec. 2003, pp. 3808 – 3812, doi: 10.1109/GLOCOM.2003.1258944

[10] Hai Le Vu, A. Zalesky, E.W.M. Wong, Z. Rosberg, S.M.H. Bilgrami, M. Zukerman, and R.S. Tucker, "Scalable performance evaluation of a hybrid optical switch", Journal of Lightwave Technology, vol. 23, Oct. 2005, pp. 2961 – 2973.

[11] Lu Kejie, Xiao Gaoxi, and I. Chlamtac, "Analysis of Blocking Probability for Distributed Lightpath Establishment in WDM Optical Networks ",IEEE/ACM Transactions on Networking, vol. 13, Feb. 2005, pp. 187-197.

[12] J. P. Jue and V. M. Vokkarane, Optical Burst Switched Networks, 1rd ed., Springer Science, 2005.

[13] C.M. Gauger, P.J. Kuhn, E.V. Breusegem, M. Pickavet, and P. Demeester, "Hybrid Optical Network Architectures: Bringing Packets and Circuits Together", IEEE Communications Magazine, vol. 44, Aug, 2006, pp. 36-42.

[14] J.P. Jue and V.M. Vokkarane, Optical Burst Switched Networks, Springer Science, 2005.

[15] A. Zalesky, "To Burst or Circuit Switch?", IEEE/ACM Transactions on Networking, vol. 17, Feb. 2009, pp. 305-318.

[16] T. Coutelen, H. Elbiaze, and B. Jaumard, "Performance comparison of OCS and OBS switching paradigms", Proc. Transparent Optical Networks, vol. 1, Jul. 2005, pp. 212-215.

[17] Liu Xin, Qiao Chunming, Yu Xiang, and Weibo Gong, "A fair packet-level performance comparison of OBS and OCS", Optical Fiber Communication Conference (OFC), 2006.

[18] C. Charoenlarpnopparut, E. Dhavarudha, and S. Runggeratigul, "Performance and Cost Comparsion for Optical Burst Switching and Optical Circuit Switchign", International Symposium on Communications and Informations Technologies, 2006.

[19] Gyu Myoung Lee, B. Wydrowski, M. Zukerman, Jun Kyun Choi, and Chuan Heng Foh, "Performance Evaluation of an Optical Hybrid Switching System", Global Telecommunications Conference, 2003.

[20] Yeshuang Wang, Sheng Wang, Shizhong Xu, and Xiufeng Wu, "A new hybrid optical network design consisting of lightpath and burst switching", Advanced Communication Technology, vol. 3, Feb. 2009, pp. 1873 -1876.

[21] P.S. Khodashenas, J. Perelló, S. Spadaro, J. Comellas, and G. Junyent, "A feedback-based hybrid OBS/OCS architecture with fast-over-slow capability",Optical Network Design and Modeling (ONDM), May 2011, pp. 1-14.

 ISBN: 978-1-61208-231-8

The Impact of Geography and Demography on the Economics of Fibre Optic Access Networks

Raquel Castro Madureira, A. M. Oliveira Duarte
Instituto de Telecomunicações, Dpt°. de Electrónica, Telecomunicações e Informática
Universidade de Aveiro, Aveiro, Portugal
rcmadureira@ua.pt

Raquel Matias-Fonseca
Dpt°. de Economia, Gestão e Eng.ª Industrial
Universidade de Aveiro, Aveiro, Portugal
rfonseca@ua.pt

Carina Pais, Jorge Carvalho
Dpt°. de Ciências Sociais, Jurídicas e Políticas
Universidade de Aveiro, Aveiro, Portugal
pais@ua.pt, jcarvalho@ua.pt

***Abstract*—This article presents a study relative to the influence that demographic and geographic conditions have on the economics of fiber optic telecommunications access networks. This approach differs from other studies by merging classical techno-economic evaluation methods with geographic engineering tools and models. This analysis is part of a project to identify the costs of all type of utilities´ infra-structures as a function of the degree of urban dispersion. The work presented in this paper is the quantification of a PON network using an approach that combines fiber optics engineering and deployment with geographic tools.**

Keywords- GPON techno-economics; access network fiber deployment; urban dispersion; local scale; utilities.

I. INTRODUCTION

Today´s cities are quite different from the past. The continuous geographical expansion of the utilities' infrastructures such as the water, the natural gas, the sewerage system, the electricity and the telecommunications [1] contributes to a generalized increasing of the quality of life and is reflected in the organization and urbanizations of the population´s settlements. In consequence from the building compactness and continuity of the old city, raises a new type of fragmented and spread urbanism.

But, if for most of the infrastructures it is likely to "follow" the inhabited settlements based on municipals master plans, the classic approach of the telecommunications operator's is to focused their deployment plans on the urban administrative limits, where is forecast a guaranteed financial return.

In parallel, the growth of the telecommunications demand requires faster and wider broadband to each house/person leading towards a new global Information and Communication Technologies (ICT) era. The fact that the United Nations (UN) considered the telecommunications broadband access an universal right [2], has increased the pressure to expand the new generation telecommunication infrastructures, namely the high speed optical networks, to all type of municipal arrangements [3]. Nowadays, the main constrains for the deployment of those types of networks is not so much the technology maturity but the civil work´s inherent costs [4] mainly in rural and exurban scattered zones.

The research described in this paper is focusing in the exurban areas where the typical profile is people with higher college education level than closer-in suburbs, people that migrate to center city during the day for work, and return home at night, far from the crowd but with interest in being "*always on line*". A correct approach to the delimitation of the extended city and the urban dispersion borders can lead to a potential new planning area and profitable business plan, by integrating a set of methodological phases from the techno-economic analysis to the geographical modeling.

Considering this, the main objective of the paper is the evaluation of the overall costs when comparing different forms of habitat (concentrated and dispersed) at the local scale at a brownfield gigabit passive optical network (GPON).

This paper is divided as follows: Section I defines the context of the paper. Section II defines the technological scenarios´ of the study. It is dedicated to the description of the optical access network architecture and respective components' cost assumptions. Section III describes a method to extract a geographical model from real data of suburban settlements of typical Portuguese medium sized cities. Section IV presents the forecast results of a gigabit passive optical network, GPON network in both urban and suburban environments obtained by applying the extracted model at the local scale to a real city. Finally, a summary is presented.

II. INITIAL ASSUMPTIONS

In the telecommunication world there are several possibilities to reach each subscriber. They can be reached either individually at their mobile phones or at each one´s house by cable (in this paper, each house/door will be referred as Dwelling Unit, DU).

The access technology elected for this study was the GPON. The reasons that lead to the choice of an optical network as the high speed provider were the wider spread of the other most common solution, as described next and also the existence of ancient technologies that provide infrastructures that can be shared and consequently reducing the costs for the migration:

- Global access to the voice service is provided on the existence of the universal service (US) for plain old

 ISBN: 978-1-61208-231-8

telephone service (POTS) and low debt internet based on Asymmetric Digital Subscriber Line (ADSL), [5-7];
- The broadcast television is also considered universal (e.g. more than 99.5% of the Portuguese population own at least one TV set [8] and 75% more than two);
- The mobile wireless subscriber penetration for both voice and data, in the context of the urban dispersion, can be considered not far from 100% (e.g. In Portugal reaches 120% [9]);

There is already in the field a fixed subterranean infrastructure that can be shared with other technologies and suppliers [10], assuming a share percentage of ducts around 50% and it is considered that most of the traditional urban and suburban areas already have a digital subscriber line (DSL) infra-structure and consequently at least one street cabinet or manhole already exists per neighborhood.

As the main focus in this work is the comparison of the local scale network, all the cost calculation will focus on the shared neighborhood infrastructure and all the access network´s segments shared among the several neighborhoods, such as the central office (CO), are excluded at this point. It is also assumed that 100% of the buildings, houses, schools and other institutions, under the limits of the urban dispersion occupation, will be equipped with optical fiber.

A. GPON Architecture at the Local Scale

Most logical architectures for the telecommunications networks are based around a system of three sets of layers. A common layer description is composed by: Core, Access and Client networks, see Figure 1.

The core network gives internetwork connectivity and interoperates with the "cloud" and other networks. The client network is the segment directly connected to the client through an electronic device depending of the technology such as a mobile phone, a TV set, a modem or a telephone, among others. The access network is the layer that connects both extremities segments and is the layer that is most often considered to the cost evaluation of a telecommunication´s network deployment, [11-13].

A fiber optical network based on a fiber to the home or building architecture (GPON FTTH/B) can be deployed in many different ways depending number of existing houses, the number of clients; the environment topology; streets rearrangement and equipment available or chosen by the engineer. In this particularly study, the network infrastructure is based on manholes, trenching ducts, or mast for aerial support of the fiber. This paper presents a redefinition of the standard concept, with a new vision of the access network infrastructure.

The local scale infrastructure: that is the part of the access network segment that is serving directly the neighborhood here referred as the base land unit, BLU. It excludes the Central Office. And the global access infrastructure is the network segment that is serving a wider territorial unit, as the whole city. It includes the core network and parts of the access networks that connects several neighborhoods or BLU´s, see Figure 1.

At this stage, it should point out the infrastructure costs of the global access infrastructure will be disregarded, not because they are irrelevant but due to the local scale perspective the global costs are equal in all cases. It is defined that all existing houses or public buildings are being deployed with fiber so the number of clients is equal to the number of existing "doors" or DU. It is also stated that each house receives 1 optical fiber.

Moreover, we also consider a fixed default architecture configuration so that the dispersion scenarios could be comparable. The FTTH/B GPON architecture chosen was based on the following considerations.
- In GPON, the maximum differential fiber distance is 20 km so the total dimension from the CO to the client cannot exceed 20Km [14];
- The optical link budget must safeguard a positive system margin ;
- It is expected that in average the length (L) of each fiber segment obeys the rule: L1<L2<L3 , see Figure 1;
- There is only one stage of passive optical splitters to distribute the fiber to each customer;
- The splitting ratio is fixed to 1:32 for all splitters;
- There can be more than one flexibility point (FP), depending of the neighborhood geometry.

B. Cost Analysis Method

The initial objective of this study is to obtain the cost comparison between several scenarios for the dispersive urban occupation, from the society point of view, as a whole. Any allocation or apportionment of costs between the telecommunication players will not be considered such as: service providers, infrastructure owners, state or subscribers. Likewise, the existence of taxes or any forms of payment mechanisms will also not be considered.

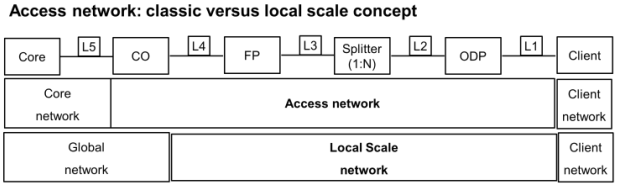


Figure 1. Telecommunication networks layers comparison with local scale concept.

The costs are reported in a reference period of 30 years. This option enables a cost / benefit analysis, since it seems reasonable with such time horizon to affect also the value of the buildings, in fact, from there on, the building requires maintenance work / reconstruction of very significant costs.

The cost of any infrastructure´s component or equipment (CT) is the sum of the Investment Cost (IC) and the Maintenance Costs (MC) in the fixed 30 year period (1).

$$CT(30years) = IC + MC \quad (1)$$

For each component or equipment, the IC includes the civil works costs plus the acquisition and installation costs of the equipment. To calculate it, it is necessary to adopt a financial annual discount rate (FDR), that according to the

European Commission (EC) should be FDR=5%, [12]. IC can then be written for a 30 year period. It is taken into account for each component, the life time, V, and the need for its replacement.

The calculation of the number of investments for each component is given by K+1, where K is an artifice for non-multiple divisions and equals abs(the roundup of 30/V-1). The first parcel of (2) reflects the sum of the initial investments needed for a certain component, depending on its time life. Each year, the initial component cost (C_i) is affected by the FDR at the calculation year (n.V).

Sometimes, the component lifetime (V) can go beyond the 30 year assumed project life time, and because of that, in the second parcel of (2) is subtracted the portion of the investment corresponding to that differential, affected by the FDR at year 30.

$$IC = \left[\sum_{n=0}^{K} \frac{C_i}{(1+FDR)^{n \cdot V}}\right] - \left[\frac{(k+1)\cdot V - 30}{V} \cdot \frac{C_i}{(1+FDR)^{30}}\right] = C_i \cdot f(V) \qquad (2)$$

Where Ci is the initial investment at year 0, V is the lifetime in years, K=abs (roundup (30/V-1; 0)) and FDR=0,05.

The maintenance costs are related to the energy consumption, periodical inspections and rents. It can be expressed based on the annual maintenance costs C_m and the FDR (5%), (3). Usually, this coefficient is described as a percentage of IC.

$$MC = \sum_{0}^{(V-1)} \frac{C_m}{(1+FDR)^n} = 16{,}14 \cdot C_m \qquad (3)$$

Where V is the lifetime in years, Cm are the maintenance costs that usually are described as a percentage of IC, %Cm and FDR=0,05.

C. GPON Investment and Expenses

The equipment prices are reported to the year 2010 and are based on data from the components suppliers found on the web. Whenever is possible the calculations are presented as a function of € per DU and if it is not possible is presented as € per meter. It is also assumed that 1 DU corresponds to 2.4 inhabitants, [15].

All the equipments and components are related to Figure 1.

1) Fibers (fo): The fiber segments are optical cables that contain several optical fibers (fo) namely groups of 288fo, 48fo or 24fo, can be buried in ducts or aerial supported on masts. In the case of buried fiber deployment, the value of civil works and ducts is assumed to be half the real price. This is due to the fact that it is assumed that at least 50% of the trenches already exist and are shared. In the case of the aerial deployment it is assumed that each mast height is around 8 m and the distance between masts is typically 50m.

If there is more than one flexibility point, FP, the L3 segment can be divided in smaller cable slots between FP´s, named L3.1 and L3.2 (from the client to the core). At L3.1 segment a 24fo cable is considered, and at L3.2 segment is assumed to have a 48fo cable. The final cable segment, L1, could be inexistent if the ODP is in the building façade. If the ODP is shared among several single houses L1 can be deployed either underground or aerial, unless the inter-house distance is economically impracticable, as will be discussed in Section IV.

Tables I and II presents the CAPEX and OPEX of the different fiber segments for the different types of deployment considered.

TABLE I FIBER COST BURIED DEPLOYMENT IN € AND PER METER

Fiber L3.2	**C_i**	**V**	**%C_m**	**f(V)**	**IC**	**MC**	**CT**
Civil work/m	25	50	2%	0,9	22.7	8.1	30.8
Equip.+ install.	2.3	20	4%	1.3	2.8	1.5	4.3
Total/m					25.5	9.6	35.1
Fiber L3.1/L2/L1	C_i	V	%C_m	f(V)	IC	MC	CT
Civil works/m	25	50	2%	0.91	22.7	8.1	30.8
Equip.+ Install.		20	4%	1.26	2.4	1.1	3.5
Total €/m					25.1	9.2	34.3

Where C_i is in €, V in years, C_m is a percentage of C_i, f(V) is a adimensional, IC, MC and CT are in €.

TABLE II - FIBER COST AERIAL DEPLOYMENT IN € AND PER METER

L3.2/L3.2/L2/L1	**C_i**	**V**	**%C_m**	**f(V)**	**IC**	**MC**	**CT**
(Mast+installation)/m	2.5	50	2%	0.9	2.4	0.8	3.2
Equipment and installation	3	20	4%	1.3	4.4	1.9	6.4
Total Cost/m					6.6	2.7	9.6

Where C_i is in €, Vin years, cm is a percentage of C_i, f(V) is a adimensional, IC, MC and CT are in €.

2) Flexibility points (FP):

The flexibility points, usually in manholes, are used to separate physically the cable in the hub corners and street cross points. They are define as 1:N type, depending on the number of cables they aggregate in one cable. In this study, FP1 is type 1:2 that means that receives 2 L3.1. cable segments from the splitters and join them into 1 cable of 48fo (L3.2). Then in 1:6 type, FP2, the process repeats and FP2 ends with 6*48=288cable (L4) of 48fo entering the CO.

Table III shows the cost of the equipment and man work for the most common installation at underground cable camber (manhole) for a 30 year analysis period.

TABLE III - FLEXIBILITY POINT COSTS PER EQUIPMENT IN €

	C_i	**V**	**%C_m**	**f(V)**	**IC**	**MC**	**CT**
Civil works	360	50	2%	0.91	328	116	444
Equip.+instal	438	30	15%	1	438	1060	1498
Total €/unit					766	1176	1942

Where C_i is in €, V in years, C_m is a percentage of C_i, f(V) is a adimensional, IC, MC and CT are in €.

3) Splitters: The splitters are power dividers usually mounted in Fiber distribution Hubs (FDH) cabinet's also known as street cabinets. The theoretical scenario of a fully occupied street cabinet with maximum capacity of 24

splitters was assumed. From the central office and after the flexibility points, each 1:32 type splitter receives a 24fo cable and divide each fiber in 32 fibers grouped in cables of 24fo. In this scenario, each splitter was able to serve 788 DU´s, if all the fibers were used for clients, however a percentage is reserved to network maintaince.

Table IV shows the cost of each cabinet with the 24 splitter stage for a 30 year analysis period.

TABLE IV - STREET CABINET WITH 24 SPLITTERS COSTS IN €

	C_i	V	%C_m	f(V)	IC	MC	CT
Cabinet and installation	2820	20	4%	1.26	3557	1821	5377
Equipment and installation	8759	15	15%	1.28	12963	21205	34168
Total Cost per cabinet of 24 splitters					16520	23025	39545

Where C_i is in €, Vin years, cm is a percentage of C_i, f(V) is a adimensional, IC, MC and CT are in €.

4) Optical Distribution Point (ODP): The ODP Box is an infrastructure component which main function is to connect the distribution network to the client and it may be mounted either indoor or outdoor. Each ODP receives a 24fo cable. In this study, it is assumed that there are no splitters inside the ODP and 4 of the 24 fibers are reserved for the telecommunications operator's maintenance issues. Each ODP is shared among an integer number of buildings or houses up to a certain inter-house distance. Table V shows the cost of each ODP at each building entrance for a 30 year analysis period.

TABLE V – OPTICAL DISTRIBUTION POINT COST IN EUROS

	C_i	V	%C_m	f(V)	IC	MC	CT
Equipment and installation	120	20	15%	1.26	151	291	442
Total cost/ODP					151	291	442

Where Ci is in €, V in years, Cm is a percentage of Ci, f(V) is a adimensional, IC, MC and CT are in €.

The following table, Table VI illustrates the multiplication factor of each component relative to the number of dwelling units served.

TABLE VI - GPON COMPONENTS MULTIPLICATIVE FACTOR

Network element	Factor	Min. use	Low use	Max. use
FP1	6	384	3840	7680
FP2	2	64	640	1280
Splitter	32	32	320	640
ODP	1 to 20	1	10	20

III. URBAN DISPERSION IDENTIFICATION METHODOLOGY

The study of urban dispersion on a local scale requires the adoption of operational concepts. This research uses the notion of "Base Land Unit" (BLU), which represents a piece of land for experimental studies [16], which will be used to characterize the land occupation by defining a BLU ranking. The recognition of BLU is more difficult in urban territories because its fragmentary and dispersive expansion dynamics are not consistent with the administrative limits.

The research project's case studies are two typical medium European types of cities. One type which is generally regarded as a concentrated city that developed (more or less) homogeneously around a nuclear old city and another type that derived from the same type of origin but for several factor grew in such a way that is usually associated to a more dispersed or diffused territory.

A. Local Scale BLU Modeling

The first approach of the land unit, LU characterization consists on the analysis of digital aerial photos to delimit the borders of the extended city, based on the maximum distances between buildings. This digital method typifies the building agglomeration in three types: continuous, dispersed and rarefied.

The Base Land Unit, BLU, concept integrates and almost coincides with other well-known territorial units, namely the neighborhood in its everyday meaning. The BLU concept differs from the neighborhood as it does not necessarily refer to an exclusively residential area – it may also encompass central or industrial areas, techno-centers, a dispersed settlement area or even an agricultural and/or forested area within the extended city.

In this study, with the focus on the local scale, a base land unit for the concentrated occupation with no more than 3000 residents and corresponding to 1200 DU´s is considered. The DU's are most of them buildings but also single houses; it also includes some green plazas and the existence of public equipments as schools, commercial zones and hospitals in a total of 133 DU´s.

The geographic applied method identified attributes to differentiate standard BLU´s scenarios to work with, [17] as building aggregation in city blocks or one-to-one; usage as uni/bi-functional versus multi-functional buildings and distance to the public equipments and commerce, among others.

The observation and quantification of these attributes lead to a classification of the Concentrate BLU in two main groups: Classic and Modernist, with each one of these classifications further divided in uni/bi-functional or multi-functional building aggregation leading to 4 types of scenarios [16]. The dispersed urbanization characterization is followed by several defined attributes that combined can formulate 9 different types of scenarios [17]. Only the three most suitable were chosen to the reality in study. These environments are characterized by groups of edifications as: linear and continuous (LC), scatter and occasional (SO) and uniform and occasional (UO).

As an example, Figure 3 illustrates the final aspect of the base land unit, concentrated classic and dispersed uniform and occasional based on the previous attributes manipulation. For the dispersed BLU occupation, it was defined an universe of 1000 inhabitants corresponding to 400 DU´s. For this type, of BLU specific taxonomy and adapted attributes were tested. The attributes adopted

 ISBN: 978-1-61208-231-8

include the linear density (LD) indicator which can be expressed by the number of houses per linear track. Its results were compared with the real environment and as a consequence a LD grade scale was defined. One of the conclusions of this indicator´s reading is that is also applicable to all type of BLUs and not only to the dispersion ones.

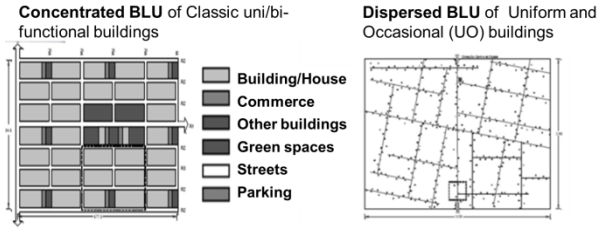


Figure 2. Sprawl scenarios: concentrated BLU of Classic uni/bi-functional buildings, on the left and Dispersed BLU-UO, on the right.

Table VII presents the summary of the main characteristics of the chosen standard scenarios.

TABLE VII - BLU STANDARD SCENARIOS

	Concentrated BLU				Dispersed BLU		
	Uni/bi-functional		Multi-functional		LC	SO	UO
	Classic	Modern	Classic	Modern			
Pop.	3000				1000		
Area (ha)	29.4	54.5	24.6	18.2	375	375	800
Building	828	1234	202	88	400		
LD (#DU/m)	19.2	10.4	28.5	40.8	7.5	5.3	1.5

Where BLU stands for Base Land Unit, LC stands for Linear and Continuous urbanizations, SO stands for Scatter and Occasional urbanizations and UO stands for Uniform and Occasional urbanizations. The area is in hectare (ha) and the Linear Dispersion (LD) is the number of DU per 100 meters of street.

IV. RESULTS

At this point, all the data presented in the previous sections is compiled. The telecommunication network´s technology and architecture were chosen; several components of a local scale optical fiber network were identified, as well their cost in a 30 years period and the urban+suburban distribution was characterized leading to two types of urban settlements: the concentrated and the disperse with several variants.

This section resumes the conclusions after applying the described techno-economic method to the geographical model and respective scenarios.

A. Architecture tips: profitable distance to share ODPs

The deployment of the optical network in all seven urban scenarios, Table VII, followed the same method. First, all the ODP were placed as close as possible to the buildings, in order to capitalize its cost in a relation with 1 ODP per 20 DU´s. The ODP´s have an output of 24 fibers, but it was assumed that 4 fibers were reserved to operator´s maintenance operations. If the scenario is not a building but several individual houses the same ODP is shared among them as long they are in the same side of the street.

At this point it is interesting to understand how long L1 can be, before the need of a second ODP considering the balance of the investment in fiber and in another ODP. The depicted variables R1 and R2 try to illustrate this theoretical situation. On the left of the image, it is shown the ideal situation of 1 ODP per building, in the middle there is the case of an ODP sharing using underground fiber and in the right there is the situation of an ODP sharing with aerial fiber, see Figure 3.

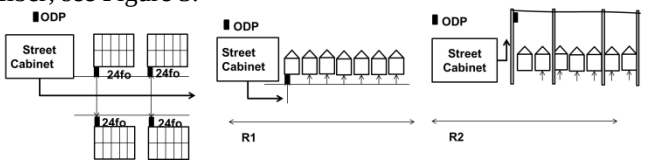


Figure 3. Testing scenarios for techno-analysis of ODP sharing: the ideal situation of 1 ODP per building (on the left), the ODP sharing with fiber underground (in the middle), ODP sharing with aerial fiber (on the right).

In a concentrated environment and according to the pattern adopted, 1 FP serves 12 cabinets and each one serves 32 ODP and the cost evaluation of the Local Scale Cost per ODP (LSCO) can be calculated as presented in (4).

$$LSCO = \frac{Cost\ FP1 + Cost\ FP2}{n^{o}\ of\ served\ ODP_1} + \frac{Cost\ per\ full\ cabinet}{n^{o}\ of\ served\ ODP_2} + ODP\ cost \qquad (4)$$

Within this perspective a first finding is that R1=49m and R2=176m is the maximum recommended L1, see Figure 1 before use another ODP. After the distribution of the ODP´s, it is necessary to place the cabinets with the splitters optimizing the L2 (it also depends on licenses and municipally authorization). And depending on it, the location for the flexibility points should be placed optimizing L3 length.

B. GPON Cost comparison per geographic model

Taking these rules into attention and deploy the chosen GPON architecture per geographic scenario it is possible to apply the developed calculation algorithm based on MSExcell to each one of the urban concentrated and dispersed settlements. A shopping list can be extracted from the calculation tool and can be seen in more detail in TABLE VIII.

As expected, the investment in infrastructure is always bigger in dispersed than in concentrated enviroment but massive saving can be done either by sharing or choose aerial deployment. This last solution is less expensive from 58% to 78% than the buried one, for 50% of ducts shared and can reach more than 85% in dispersed uniform and occasional settlements if there is a 100% sharing.

V. CONCLUSIONS

The deployment of broadband networks is one of the target measures of several governments and entities in many countries around the world. In some geographic areas, it can be interpreted as an answer to the market demand for new

 ISBN: 978-1-61208-231-8

and attractive high speed applications; in other areas it is seen as a seed of development. One relevant fact is that this dichotomy is shared among many countries, ranging from the most industrialized to the emerging economies, meaning that in most of the countries both situations can be found. In fact, there is a widespread understanding that the access to broadband is a factor of society's equitable opportunities. However, the cost is still a drawback and investments should be done wisely.

This paper presented the quantification of a PON network using an approach that combines fiber optics engineering and deployment with geographic tools. This analysis was focused at the local neighborhood level, taking into consideration urban and exurban scenarios modeled by the geographical method.

This analysis is part of a project made with several departments, to identify the costs of all type of infra-structures as a function of the degree of urban dispersion (telecommunications, gas, water, sewage, garbage collection, electricity and public lightning) based on the characterization of two Portuguese medium sized cities. The main objective of the global project is to attribute a cost value per DU in a modern city and surroundings as a guideline to future concerted territorial planning policy.

ACKNOWLEDGMENT

Raquel Castro Madureira acknowledges Fundação da Ciência e da Tecnologia, FCT for the PhD Grant SFRH/BD/62087/2009.

This work package was done under the project "Ocupação Dispersa" supported by the Fundação da Ciência e da Tecnologia PTDC/AUR/64086/2006.

TABLE VIII– COST ELEMENTS FOR PASSIVE OPTICAL NETWORK STANDARD BASE LAND UNIT SCENARIOS WITH 50% DUCT SHARING

50%duct sharing	**Concentrated BLU**				**Dispersed BLU**					
Usage	**Uni/bi-functional**		**Multi-functional**		**Linear and Continuous**		**Scatter and Occasional**		**Uniform and Occasional**	
Scenarios	**Classic**	**Modernist**	**Classic**	**Modernist**	**Under.**	**Aerial**	**Under.**	**Aerial**	**Under.**	**Aerial**
#ODP	92	66	72	92	23		27		23	
#Cabinets (24 splitters)	3	2	3	3	1		3		4	
#FP	2	2	2	2	2		2		2	
L1 (*m*)	5402	20844	3120	0	12654	33856	13938	35800	54996	64400
L2 (*m*)	5043	4536	3645	3572	4367		3651		10535	
L3.1 (*m*)	384	369	267	143	236		290		150	
L3.2 (*m*)	365	360	542	326	50		3755		1855	
Cost (€ /DU)	450€	890€	330€	230€	1700€	920€	2250€	1030€	6700€	1990€
% Civil works	63%	80%	57%	42%	70%	90%	68%	90%	75%	90%
%Equipment	37%	20%	43%	58%	30%	10%	32%	10%	25%	10%

REFERENCES

[1] Portuguese Law / Lei nº23/96 - Essential utilities, 1996, D.R n.º 172 (Série I), pp.2108.

[2] U. Nations, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," Human Rights Council2011.

[3] CE. (2009, IP/08/1397 - Broadband Internet for all Europeans: Commission launches debate on future of universal service. Europa Press Release Rapid on line.

[4] F. C. Europe. (2010). FTTH Business Guide. Available on line: http://www.ftthcouncil.eu/

[5] Decree-Law/ Decreto Lei 91/97 - Lei de Bases das Telecomunicações DR, 1997, pp.4010.

[6] ANACOM, "Regulator statistics, fixed telephone - 4th quarter 2010," 2010, on line www.anacom.pt..

[7] R. C. Madureira, A. M. O. Duarte, and R. Matias-Fonseca, "133 years of Telecommunications Universal Service in Portugal " in HISTELCON'2010 Madrid, Spain 2010, pp. 1-6.

[8] Obercom. (2008). Portuguese TV access in 2008 (available in Portuguese). Available: http://tvdigital.files.wordpress.com/2008/09/obercom-acesso-tv-2008.pdf

[9] ANACOM, "Regulator statistics, mobile telephone - 4th quarter 2010," 2010, on line www.anacom.pt.

[10] P. Telecom. (2010). Reference Offer to Ducts Access (available in Portuguese). Available on line: //ptwholesale.telecom.pt/

[11] A. V. Pardillo, "Aplicatión del análisis tecno-econnómico al despliegue de redes de acceso de próxima generación. El caso de la competencia entre plataformas, la regulación y las políticas públicas en España," PhD, Escuela Técnica Superior de Inginieros de Telecomunicatión, Universidad Politecnica de Madrid Madrid, 2011.

[12] K. Casier, "Techno-economics of FTTH deployment in the presence of competition," PhD, Faculteit Ingenieurswetenschappen Vakgroep Informatietechnologie, Universiteit Gent, Gent, 2010.

[13] S. E. T. Halldor Matthias Sigurdsson, Thomas K. Stidsen, "Cost Optimization Methods in the Design of Next Generation Networks," IEEE Communications Magazine, 2004.

[14] ITU-T, "ITU-T G.983.1 " in Broadband optical access systems based on Passive Optical Networks (PON), ed, 2005.

[15] I. N. d. E. I. Statistics Portugal. (2011). CENSOS 2011. Available: on line: http://censos.ine.pt/

[16] J. Carvalho, Book to be edited "Ocupação Dispersa- Custos e Benefícios, à Escala Local "(available in Portuguese), 2011.

[17] J. Carvalho and C. Pais, "Methodology to Identify Dispersed Occupation on a Local Scale," presented at the Cittá 3nd Annual Conference on Planning Research, Faculdade de Engenharia da Universidade do Porto, 2009.

 ISBN: 978-1-61208-231-8

Asynchronous Sequential Symbol Synchronizers based on Pulse Comparison by Positive Transitions at Bit Rate

Antonio D. Reis[1,2] and José P. Carvalho[1]
Dep. Física / Unidade D. Remota
[1]Universidade da Beira Interior, 6200 Covilhã, Portugal
adreis@ubi.pt, pacheco@ubi.pt

José F. Rocha[2] and Atilio S. Gameiro[2]
Dep. Electrónica e Telecom. / Instituto Telecom.
[2]Universidade de Aveiro, 3810 Aveiro, Portugal
frocha@det.ua.pt, amg@det.ua.pt

***Abstract*- This work studies the asynchronous sequential symbol synchronizers based on pulse comparison by positive transitions at rate (ap). Their performance will be compared with the reference asynchronous symbol synchronizers based on pulse comparison by both transitions at rate (ab). For the reference and proposed variants, we consider two versions which are the manual (m) and the automatic (a). The objective is to study the four synchronizers and evaluate their output jitter UIRMS (Unit Interval Root Mean Square) versus input SNR (Signal Noise Ratio).**

Keywords - Synchronism; Digital Communications

I. INTRODUCTION

This work studies the asynchronous sequential symbol synchronizer based on pulse comparison operating by positive transitions at rate (ap). Their jitter is compared with the reference asynchronous synchronizers operating by both transitions at rate (ab) [1, 2].

For both, reference and proposed variant, we consider the versions manual (m) and automatic (a) [3, 4, 5, 6, 7].

The difference between the reference and proposed synchronizer is in the symbol phase comparator since the others blocks are similar. The phase comparator compares the input variable pulse duration Pv with the intern reference fixed pulse duration Pf and the error pulse Pe synchronizes the VCO (Voltage Controlled Oscillator) [8, 9].

The synchronizer regenerates the data, recovering a clock (VCO) that samples and retimes the data [10, 11, 12, 13].

Fig. 1 shows the blocks of the general symbol synchronizer.

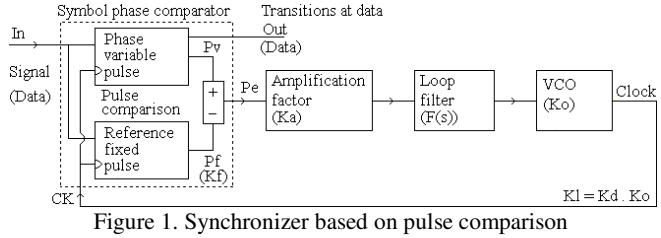


Figure 1. Synchronizer based on pulse comparison

Following, we present the reference variant, asynchronous sequential symbol synchronizers based on pulse comparison by both transitions at rate, with versions manual (ab-m) and automatic (ab-a). Next, we present the proposed variant, asynchronous sequential symbol synchronizer based on pulse comparison by positive transitions at rate, with versions manual (ap-m) and automatic (ap-a).

After, we present the design and tests. Then, we present the results. Finally, we present the conclusions.

II. ANTERIOR WORK AND NEW CONTRIBUTIONS

While various types of synchronizers were developed, very little has done on evaluating their quality.

The motivation of this work is to create new synchronizers and to evaluate their performance with noise. This contribution increases the knowledge about synchronizers.

Before, we presented various synchronous synchronizers, now, we will present the asynchronous synchronizers [1,2,3].

III. REFERENCE BY BOTH AT RATE

The reference, asynchronous sequential symbol synchronizers based on pulse comparison operating by both transitions at bit rate has two versions which are the manual (ab-m) and the automatic (ab-a) [1, 2].

The versions difference is in the phase comparator, the variable pulse Pv is common but the fixed Pf is different.

A. Reference by both at rate manual (ab-m)

The block Pv, shown below, produces a variable pulse Pv between the input bits and VCO. The manual adjustment delay with Exor produces a manual fixed pulse Pf (Fig. 2).

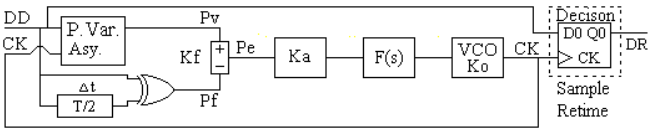


Figure 2 Asynchronous by both at rate and manual (ab-m)

The comparison between the pulses Pv and Pf provides the error pulse Pe that forces the VCO to synchronize the input. The block Pv is an asynchronous circuit (Fig. 3).

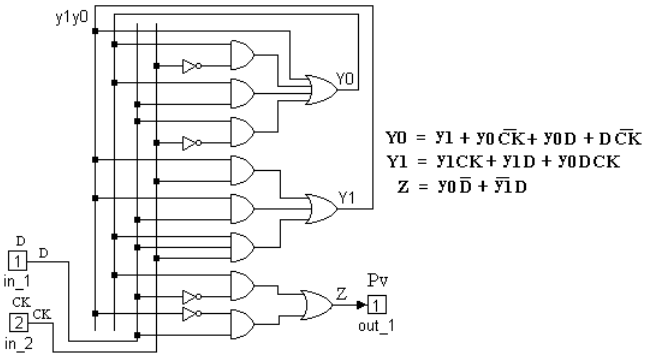


Figure 3. Intern aspect of the block Pv

Fig. 4 shows the waveforms of the reference manual (equal to the corresponding synchronous by both at rate) [3].

 ISBN: 978-1-61208-231-8

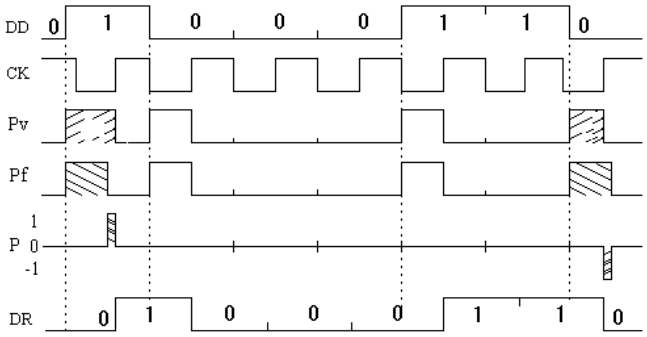


Figure 4. Waveforms of the asynchronous by both at rate manual

The error pulse Pe diminishes during the synchronization time and disappear at the equilibrium point.

B. Reference by both at rate automatic (ab-a)

The block Pv, common with anterior, produces the variable pulse Pv between input and VCO. The block Pf, shown below, produces the comparison fixed pulse Pf (Fig. 5).

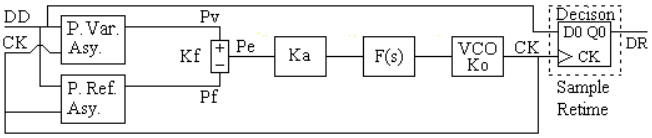


Figure 5. Asynchronous by both at rate and automatic (ab-a)

The comparison between the pulses Pv and Pf provides the error pulse Pe that forces the VCO to follow the input. The block Pf is an asynchronous circuit (Fig. 6).

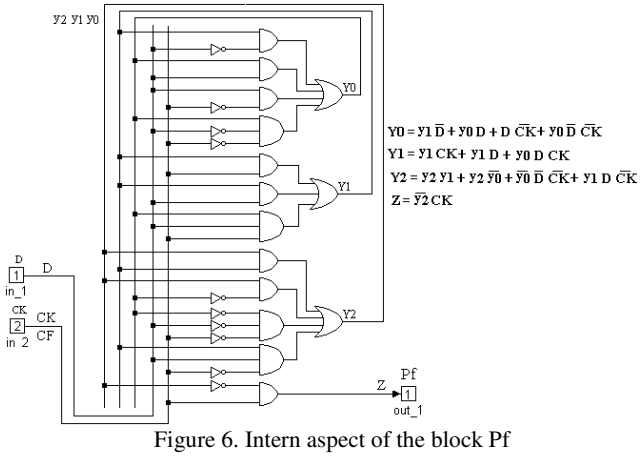


Figure 6. Intern aspect of the block Pf

Fig. 7 shows the waveforms of the reference automatic (equal to the corresponding synchronous by both at rate) [3].

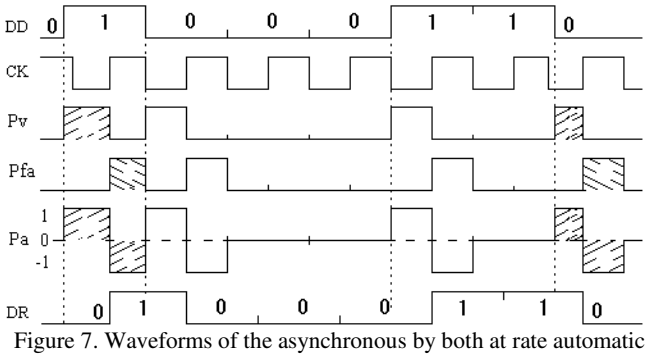


Figure 7. Waveforms of the asynchronous by both at rate automatic

The error pulse Pe does not disappear, but the variable area Pv is equal to the fixed Pf at the equilibrium point.

IV. PROPOSED BY POSITIVE AT RATE

The proposed, asynchronous sequential symbol synchronizers based on pulse comparison operating by positive transitions at bit rate has also two versions namely the manual (ap-m) and the automatic (ap-a) [3, 4].

The versions difference is in the phase comparator, the variable pulse Pvp is common but the fixed Pfp is different.

A. Proposed by positive at rate manual (ap-m)

The block Pvp produces the variable pulse Pvp between input positive transitions and VCO. The manual adjustment delay T/2 with AND produces a fixed pulse Pfp (Fig. 8).

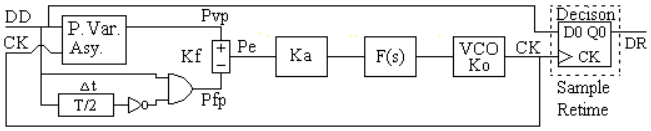


Figure 8. Asynchronous by positive at rate and manual (ap-m)

The comparison between pulses Pvp and Pfp provides the error pulse Pe that forces the VCO to synchronize the input. The block Pvp is an asynchronous circuit (Fig. 9).

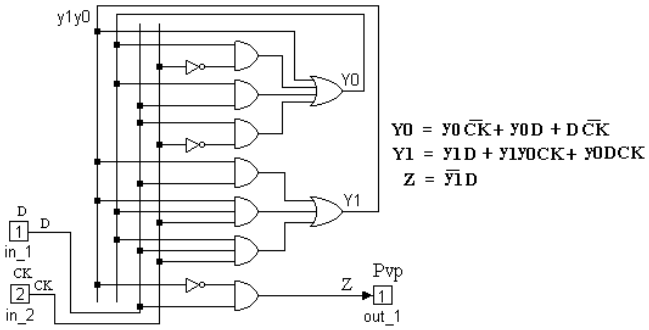


Figure 9. Intern aspect of the block Pvp

Fig. 10 shows the waveforms of the proposed manual (equal to the corresponding synchronous version) [3].

 ISBN: 978-1-61208-231-8

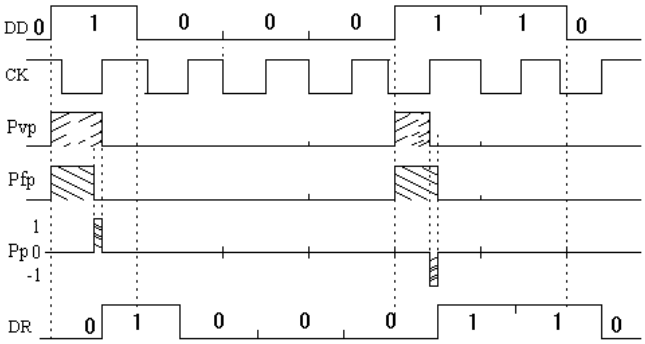


Figure 10. Waveforms of the asynchronous positive at rate manual

The error pulse Pe diminishes during the synchronization time and disappear at the equilibrium point.

B. Proposed by positive at rate automatic (ap-a)

The block Pvp, common, produces the variable pulse Pvp between input and VCO. The block Pfp, shown below, produces the comparison fixed pulse Pfp (Fig. 11).

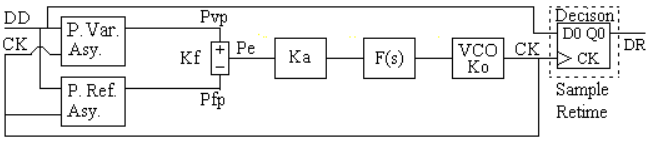


Figure 11. Asynchronous by positive at rate and automatic (ap-a)

The comparison between the pulses Pvp and Pfp provides the error pulse Pe that forces the VCO to follow the input. The block Pfp is an asynchronous circuit (Fig. 12).

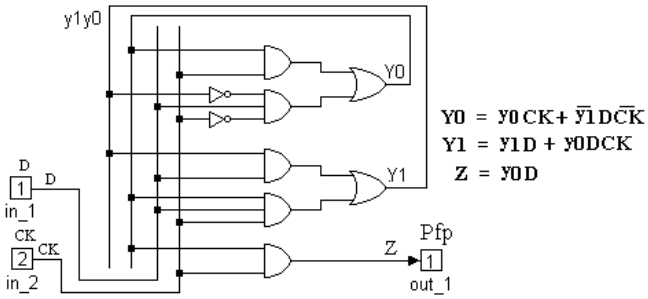


Figure 12. Intern aspect of the block Pfp

Fig. 13 shows the waveforms of the proposed automatic (equal to the corresponding synchronous version) [3].

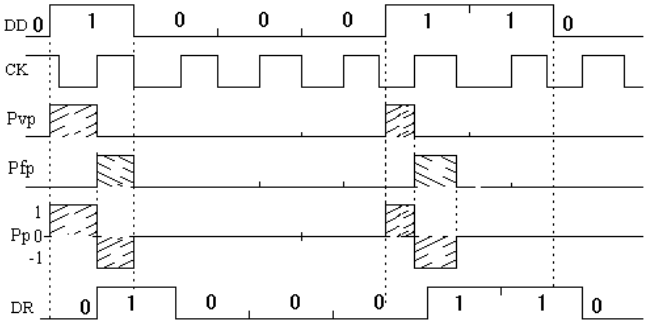


Figure13. Waveforms of the asynchronous positive at rate automatic

The error pulse Pe does not disappear, but the variable area Pv is equal to the fixed Pf at the equilibrium point.

V. DESIGN, TESTS AND RESULTS

We present the design, tests and results of the various synchronizers [5].

A. Design

To have guaranteed results, is necessary to dimension all the synchronizers with equal conditions. Then, the loop gain Kl=KdKo=KaKfKo must be equal in all the synchronizers. The phase detector gain Kf and the VCO gain Ko are fixed. Then, the loop gain amplification Ka controls the root locus and consequently the loop characteristics.

For analysis facilities, we use normalized values for the transmission rate tx=1baud, clock frequency fCK=1Hz, extern noise bandwidth Bn=5Hz and loop noise bandwidth Bl=0.002Hz. Then, we apply a signal power Ps= A^2_{ef} and a noise power Pn= No= $2\sigma n^2.\Delta\tau$, where σn is the noise standard deviation and $\Delta\tau$ =1/fSamp is the sampling period. The relation between SNR and noise variance σn^2 is

$$SNR= A^2_{ef}/(No.Bn) = 0.5^2/(2\sigma n^2*10^{-3}*5)= 25/\sigma n^2 \quad (1)$$

Now, for each synchronizer, is necessary to measure the output jitter UIRMS versus the input SNR

- 1st order loop:

We use a cutoff loop filter F(s) = 0.5Hz, is 25 times greater than Bl= 0.002Hz, what eliminates the high frequency but maintain the loop characteristics. The transfer function is

$$H(s)=\frac{G(s)}{1+G(s)}=\frac{KdKoF(s)}{s+KdKoF(s)}=\frac{KdKo}{s+KdKo} \quad (2)$$

the loop noise bandwidth is

$$Bl=\frac{KdKo}{4}=Ka\frac{KfKo}{4}=0.02Hz \quad (3)$$

So, with (Km=1, A=1/2, B=1/2, Ko=2π) and loop bandwidth Bl=0.002, we obtain respectively the Ka, for analog, hybrid, combinational and sequential synchronizers, then

$$Bl=(Ka.Kf.Ko)/4 = (Ka.Km.A.B.Ko)/4 \rightarrow Ka=0.08*2/\pi \quad (4)$$

$$Bl=(Ka.Kf.Ko)/4 = (Ka.Km.A.B.Ko)/4 \rightarrow Ka=0.08*2.2/\pi \quad (5)$$

$$Bl=(Ka.Kf.Ko)/4 = (Ka*1/\pi*2\pi)/4 \rightarrow Ka=0.04 \quad (6)$$

$$Bl=(Ka.Kf.Ko)/4 = (Ka*1/2\pi*2\pi)/4 \rightarrow Ka=0.08 \quad (7)$$

For the analog PLL, the jitter is

$$\sigma_\phi^2=Bl.No/Aef^2=0.02*10^{-3}*2\sigma n^2/0.5^2=16*10^{-5}.\sigma n^2 \quad (8)$$

For the others PLLs, the jitter formula is more complicated.

- 2nd order loop:

Is not used here, but provides similar results.

B. Tests

We used the following setup to test synchronizers (Fig. 14)

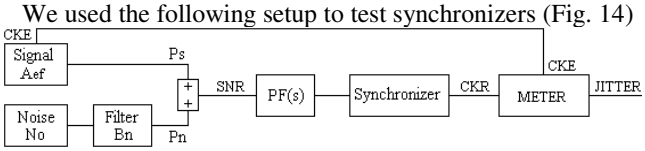


Figure 14. Blocks diagram of the test setup

The receiver recovered clock with jitter is compared with the emitter original clock, the difference is the jitter.

C. Results

We present the results in terms of output jitter UIRMS versus input SNR. Fig. 15 shows the jitter - SNR curves of the four synchronizers which are the both manual (ab-m), the both automatic (ab-a), the positive manual (ap-m) and the positive automatic (ap-a).

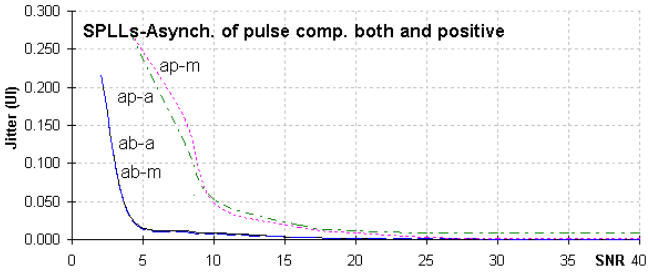


Figure15. Jitter-SNR curves of the 4 synchronizers (ab-m,ab-a,ap-m, ap-a)

We observe that, in general, the output jitter UIRMS decreases gradually with the input SNR increasing.

We verify that, for high SNR, the four jitter curves tend to be similar. However, for low SNR, the variant asynchronous both at rate manual (ab-m) and automatic (ab-a) are better than the variant asynchronous positive at rate manual (ap-m) and automatic (ap-a).

V. CONCLUSION AND FUTURE WORK

We studied four synchronizers involving the reference variant asynchronous by both transitions at rate with versions manual (ab-m) and automatic (ab-a) and the proposed variant asynchronous by positive transitions at rate with versions manual (ap-m) and automatic (ap-a). Then, we tested and compared their jitter - SNR curves.

We observed that, in general, the output UIRMS jitter curves decrease gradually with the input SNR increasing.

We verified that, for high SNR, the four synchronizers jitter curves tend to be similar, this is comprehensible since all the synchronizers are digital, with equal noise margin. However, for low SNR, the variant asynchronous by both at rate with its versions manual (ab-m) and automatic (ab-a) is better than the variant asynchronous by positive at rate with its versions manual (ap-m) and automatic (ap-a), this is comprehensible because the variant by both transitions has more transitions (double) than the variant by positive transitions and then, the going time from the error state to the correct state is lesser.

In the future, we are planning to extend the present study to other types of synchronizers.

ACKNOWLEDGMENT

The authors are grateful to the program FCT (Foundation for sCience and Technology) / POCI2010.

REFERENCES

[1] Jean C. Imbeaux, “performance of the delay-line multiplier circuit for clock and carrier synchronization in Digital Satellite Communications”, IEEE Journal on Selected Areas in Communications pp. 82-95 Jan. 1983.

[2] Werner Rosenkranz, “Phase Locked Loops with limiter phase detectors in the presence of noise”, IEEE Transactions on Communications com-30 Nº10 pp. 2297-2304. Oct 1982.

[3] Hans H. Witte, “A Simple Clock Extraction Circuit Using a Self Sustaining Monostable Multivibrator Output Signal”, Electronics Letters, Vol.19, Is.21, pp. 897-898, Oct 1983.

[4] Charles R. Hogge, “A Self Correcting Clock Recovery Circuit”, IEEE Transactions on Electron Devices pp. 2704-2706 Dec 1985.

[5] Antonio D. Reis, Jose F. Rocha, Atilio S. Gameiro and Jose P. Carvalho “A New Technique to Measure the Jitter”, Proc. III Conf. on Telecommunications pp. 64-67 FFoz-PT 23-24 Apr .2001.

[6] Marvin K. Simon and William C. Lindsey, “Tracking Performance of Symbol Synchronizers for Manchester Coded Data”, IEEE Transactions on Communications Vol. com-2.5 Nº4, pp. 393-408, April 1977.

[7] Jeffrey B. Carruthers, D. D. Falconer, H. M. Sandler and L. Strawczynski, “Bit Synchronization in the Presence of Co-Channel Interference”, Proc. Conf. on Electrical and Computer Engineering pp. 4.1.1-4.1.7, Ottawa-CA 3-6 Sep. 1990.

[8] Johannes Huber and Weilin Liu “Data-Aided Synchronization of Coherent CPM-Receivers” IEEE Transactions on Communications Vol.40 Nº1, pp. 178-189, Jan. 1992.

[9] Antonio A. D’Amico, Aldo N. D’Andrea and Ruggero Reggianni, “Efficient Non-Data-Aided Carrier and Clock Recovery for Satellite DVB at Very Low SNR”, IEEE Jou. on Sattelite Areas in Comm. Vol.19 Nº12 pp. 2320-2330, Dec. 2001.

[10] Rostislav Dobkin, Ran Ginosar and Christos P. Sotiriou “Data Synchronization Issues in GALS SoCs”, Proc. 10th International Symposium on Asynchronous Circuits and Systems, pp. CD-Ed., Crete-Greece 19-23 Apr. 2004.

[11] N. Noels, H. Steendam and M. Moeneclaey, “Effectiveness Study of Code-Aided and Non-Code-Aided ML-Based Feedback Phase Synchronizers”, Proc. IEEE Intern. Conference on Communications (ICC’06) pp. 2946-2951, Istambul-TK, 11-15 Jun 2006.

[12] Antonio D. Reis, Jose F. Rocha, Atilio S. Gameiro and Jose P. Carvalho “Sequential Symbol Synchronizers based on Clock Sampling of Discrete Pulses”, Proc. VIII Symposium on Enabling Optical Network and Sensors (SEONs) pp. CD-Edited, Porto-PT 25-25 June 2010.

[13] Antonio D. Reis, Jose F. Rocha, Atilio S. Gameiro and Jose P. Carvalho “Carrier Phase Lock Loop and Bit Phase Lock Loop”, Proc. IX Symposium on Enabling Optical Network and Sensors (SEONs) pp. CD-Edited, Aveiro-PT 1-1 July 2011.

 ISBN: 978-1-61208-231-8

Prefilter Bandwidth Effects in Asynchronous Sequential Symbol Synchronizers based on Pulse Comparison by Positive Transitions at Bit Rate

Antonio D. Reis[1,2] and José P. Carvalho[1]
Dep. Física / Unidade D. Remota
[1]Universidade da Beira Interior, 6200 Covilhã, Portugal
adreis@ubi.pt, pacheco@ubi.pt

José F. Rocha[2] and Atílio S. Gameiro[2]
Dep. Electrónica e Telecom. / Instituto Telecom.
[2]Universidade de Aveiro, 3810 Aveiro, Portugal
frocha@det.ua.pt, amg@det.ua.pt

***Abstract*- This work studies the prefilter bandwidth effects in four asynchronous sequential symbol synchronizers. We consider three prefilter bandwidths namely B1=∞, B2=2.tx and B3=1.tx, where tx is the bit rate. The synchronizer has two variants one asynchronous by both transitions at rate and other asynchronous by positive transitions at rate. Each variant has two versions namely the manual and the automatic. The objective is to study the prefilter with the four synchronizers and to evaluate their output jitter UIRMS (Unit Interval Root Mean Square) versus input SNR (Signal Noise Ratio).**

Keywords - Prefilter; Synchronizers; Communication systems.

I. INTRODUCTION

This work studies the prefilter bandwidth effects on the jitter-SNR behavior of four sequential symbol synchronizers.

The prefilter, applied before the synchronizer, switches their bandwidth between three values namely first B1=∞, after B2=2.tx and next B3=1.tx, where tx is the bit rate.

The synchronizer has four versions supported in two variants, one asynchronous by both transitions at rate with versions manual (ab-m) and automatic (ab-a) and other asynchronous by positive transitions at rate with versions manual (ap-m) and automatic (ap-a) [1, 2, 3, 4, 5, 6].

The difference between the four synchronizers is in the phase comparator. The clock is the VCO (Voltage Controlled Oscillator) that samples appropriately and retimes correctly the input data, guarantying good quality [7, 8, 9, 10, 11, 12].

Fig. 1 shows the prefilter followed of the synchronizer.

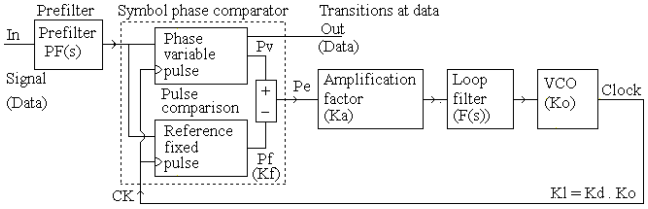


Figure 1. Prefilter with synchronizer based on pulse comparison

PF(s) is the prefilter (low pass). The synchronizer has various blocks, namely Kf is the phase detector gain, F(s) is the loop filter, Ko is the VCO gain and Ka is the loop gain factor that controls the root locus and loop characteristics.

Following, we present the prefilter with their three different decreasing bandwidths (B1=∞, B2=2.tx, B3=1.tx).

After, we present the standard reference variant, asynchronous sequential symbol synchronizers based on pulse comparison by both transitions at rate, with versions manual (ab-m) and automatic (ab-a).

Next, we present the new proposed variant, asynchronous sequential symbol synchronizers based on pulse comparison by positive transitions at rate, with versions manual(ap-m) and automatic (ap-a). After, we present the design and tests. Then, we present the results. Finally, we present the conclusions.

II. ART STATE, PROBLEMS AND SOLUTION

In the past art state was developed various synchronizers, but now is necessary to study their performance.

Previously, we studied the prefilter effects in synchronous synchronizers, the actual motivation is to study the prefilter but in asynchronous synchronizers [1, 2, 3, 4, 5].

The problem is that the jitter increases with the noise. So, to solve this problem, we propose a prefilter that attenuates the noise but however distorts slightly the signal [6, 7, 12].

II. PREFILTER BANDWIDTH EFFECTS

The prefilter, applied before the synchronizer, filters the noise but distorts slightly the signal. The prefilter bandwidth B switches between three values (B1=∞, B2=2.tx, B3=1.tx).

Fig. 2 shows the prefilter with their three bandwidths.

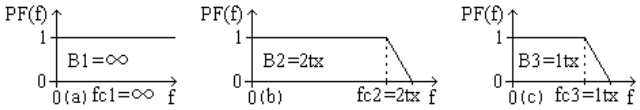


Figure 2. Three prefilter bandwidths: a) B1=∞; b) B2=2.tx; c) B3=1.tx

We will evaluate the three bandwidth effects (B1, B2, B3) on the jitter-SNR curves of the four symbol synchronizers.

a) Prefilter bandwidth equal infine (B1=∞): first (Fig.2a), we study this bandwidth effects.

b) Prefilter bandwidth equal two tx (B2=2.tx): second (Fig.2b), we study this bandwidth effects.

c) Prefilter bandwidth equal one tx (B3=1.tx): third (Fig.2c), we study this bandwidth effects.

III. REFERENCE BY BOTH AT RATE

The reference, asynchronous sequential symbol synchronizers based on pulse comparison operating by both transitions at bit rate has two versions which are the manual (ab-m) and the automatic (ab-a) [1, 2].

The versions difference is in the phase comparator, the variable pulse Pv is common but the fixed Pf is different.

 ISBN: 978-1-61208-231-8

A. Reference by both at rate manual (ab-m)

The block Pv, shown below, produces a variable pulse Pv between the input bits and VCO. The manual adjustment delay with Exor produces a manual fixed pulse Pf (Fig. 3).

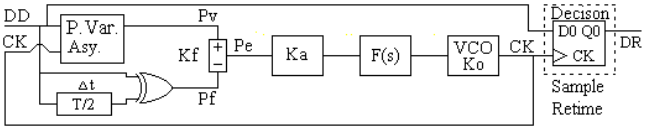


Figure 3. Asynchronous by both at rate and manual (ab-m)

The comparison between the pulses Pv and Pf provides the error pulse Pe that forces the VCO to synchronize the input. The block Pv is an asynchronous circuit (Fig.4).

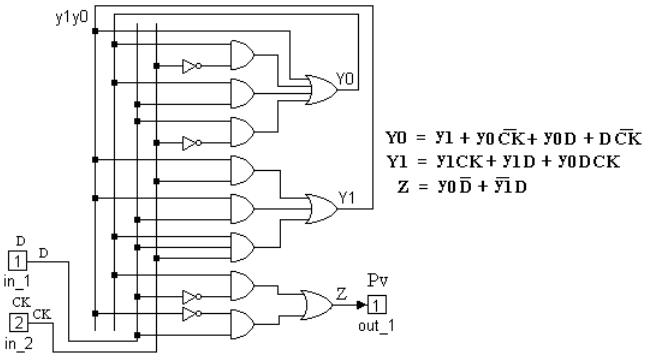


Figure 4. Intern aspect of the block Pv

The error pulse Pe diminishes during the synchronization time and disappear at the equilibrium point.

B. Reference by both at rate automatic (ab-a)

The block Pv, common with anterior, produces the variable pulse Pv between input and VCO. The block Pf, shown below, produces the comparison fixed pulse Pf (Fig. 5).

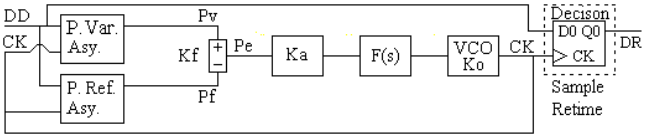


Figure 5. Asynchronous by both at rate and automatic (ab-a)

The comparison between the pulses Pv and Pf provides the error pulse Pe that forces the VCO to follow the input. The block Pf is an asynchronous circuit (Fig. 6).

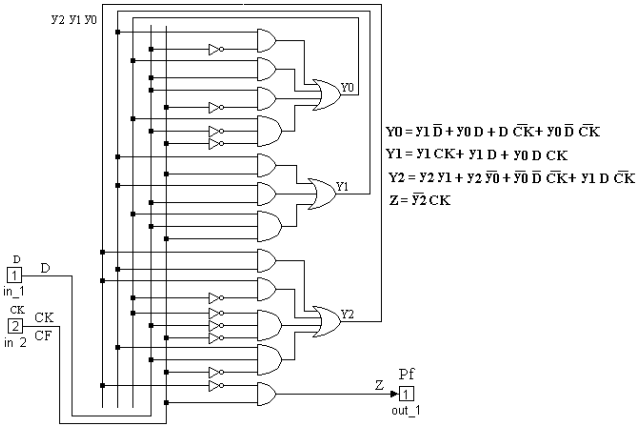


Figure 6. Intern aspect of the block Pf

The error pulse Pe does not disappear, but the variable area Pv is equal to the fixed Pf at the equilibrium point.

IV. PROPOSED BY POSITIVE AT RATE

The proposed, asynchronous sequential symbol synchronizers based on pulse comparison operating by positive transitions at bit rate has also two versions namely the manual (ap-m) and the automatic (ap-a) [3, 4].

The versions difference is in the phase comparator, the variable pulse Pvp is common but the fixed Pfp is different.

A. Proposed by positive at rate manual (ap-m)

The block Pvp produces the variable pulse Pvp between input positive transitions and VCO. The manual adjustment delay T/2 with AND produces a fixed pulse Pfp (Fig. 7).

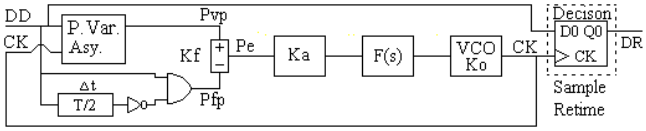


Figure7. Asynchronous by positive at rate and manual (ap-m)

The comparison between pulses Pvp and Pfp provides the error pulse Pe that forces the VCO to synchronize the input. The block Pvp is an asynchronous circuit (Fig. 8).

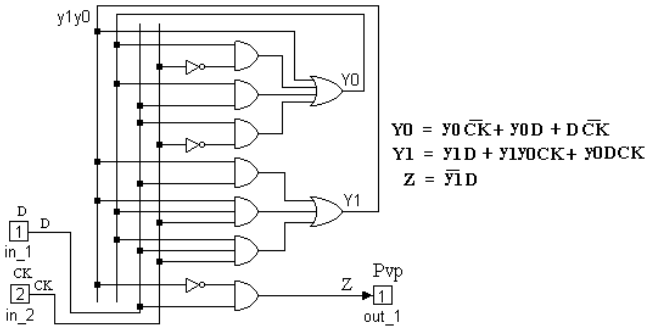


Figure 8. Intern aspect of the block Pvp

The error pulse Pe diminishes during the synchronization time and disappear at the equilibrium point.

 ISBN: 978-1-61208-231-8

B. Proposed by positive at rate automatic (ap-a)

The block Pvp, common, produces the variable pulse Pvp between input and VCO. The block Pfp, shown below, produces the comparison fixed pulse Pfp (Fig. 9).

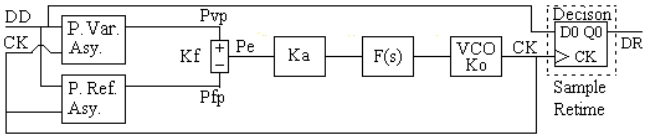


Figure 9 Asynchronous by positive at rate and automatic (ap-a)

The comparison between the pulses Pvp and Pfp provides the error pulse Pe that forces the VCO to follow the input. The block Pfp is an asynchronous circuit (Fig. 10).

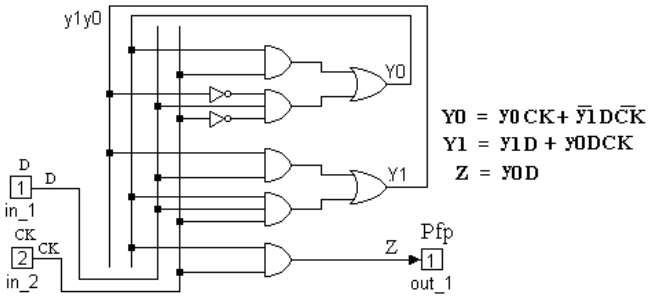


Figure 10. Intern aspect of the block Pfp

The error pulse Pe does not disappear at the equilibrium point, but the variable area Pv becomes equal to the fixed Pf.

V. DESIGN, TESTS AND RESULTS

We present the design, tests and results of the various synchronizers [5].

A. Design

To get guaranteed results, is necessary to dimension all the synchronizers with equal conditions. Then, the loop gain Kl=KdKo=KaKfKo must be equal in all the synchronizers. The phase detector gain Kf and the VCO gain Ko are fixed. Then, the loop gain amplification Ka controls the root locus and consequently the loop characteristics.

For analysis facilities, we use normalized values for the bit rate tx=1baud, clock frequency fCK=1Hz, extern noise bandwidth Bn=5Hz and loop noise bandwidth Bl=0.002Hz. Then, we apply a signal power Ps= A^2_{ef} and a noise power Pn= No= $2\sigma n^2.\Delta\tau$, where σn is the noise standard deviation and $\Delta\tau$ =1/fSamp is the sampling period. The relation between SNR and noise variance σn^2 is

$$SNR = A^2_{ef}/(No.Bn) = 0.5^2/(2\sigma n^2 * 10^{-3} * 5) = 25/\sigma n^2 \quad (1)$$

Now, for each synchronizer, is necessary to measure the output jitter UIRMS versus input SNR

- 1st order loop:

The used cutoff loop filter F(s)=0.5Hz, is 25 times greater than Bl= 0.002Hz, what eliminates the high frequency but maintain the loop characteristics. The transfer function is

$$H(s)=\frac{G(s)}{1+G(s)}=\frac{KdKoF(s)}{s+KdKoF(s)}=\frac{KdKo}{s+KdKo} \quad (2)$$

the loop noise bandwidth is

$$Bl=\frac{KdKo}{4}=Ka\frac{KfKo}{4}=0.02Hz \quad (3)$$

So, with (Km=1, A=1/2, B=1/2, Ko=2π) and loop bandwidth Bl=0.002, we obtain respectively the Ka, for analog, hybrid, combinational and sequential synchronizers, then

$$Bl=(Ka.Kf.Ko)/4 = (Ka.Km.A.B.Ko)/4 \rightarrow Ka=0.08*2/\pi \quad (4)$$

$$Bl=(Ka.Kf.Ko)/4 = (Ka.Km.A.B.Ko)/4 \rightarrow Ka=0.08*2.2/\pi \quad (5)$$

$$Bl=(Ka.Kf.Ko)/4 = (Ka*1/\pi*2\pi)/4 \rightarrow Ka=0.04 \quad (6)$$

$$Bl=(Ka.Kf.Ko)/4 = (Ka*1/2\pi*2\pi)/4 \rightarrow Ka=0.08 \quad (7)$$

For the analog PLL, the jitter is

$$\sigma_\phi^2=Bl.No/Aef^2=0.02*10^{-3}*2\sigma n^2/0.5^2=16*10^{-5}.\sigma n^2 \quad (8)$$

For the others PLLs, the jitter formula is more complicated.

- 2nd order loop:

Is not used here, but provides similar results.

B. Tests

We used the following setup to test synchronizers (Fig. 11)

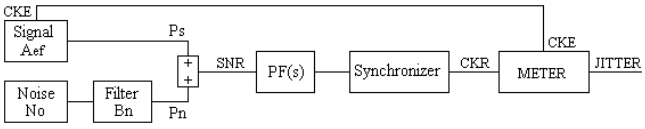


Figure 11. Block diagram of the test setup

The receiver recovered clock with jitter is compared with the emitter original clock, the difference is the jitter.

C. Results

We will present the results, in terms of jitter - SNR, for each prefilter bandwidth with the four synchronizers.

Fig. 12 shows the jitter-SNR curves for the prefilter bandwidth B1=∞ with the four synchronizers (ab-m, ab-a, ap-m, ap-a).

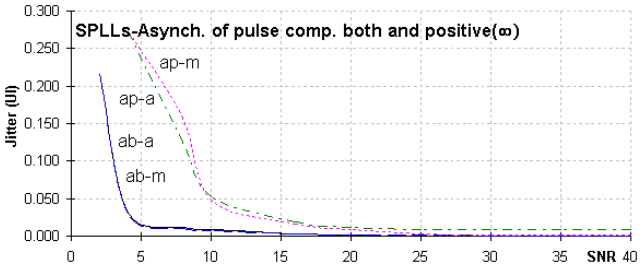


Figure 12. Jitter-SNR curves of B1+4synchronizers (ab-m, ab-a, ap-m, ap-a)

For prefilter B1=∞, we verify that, for high SNR, the four synchronizer jitter-SNR curves tend to be similar. However, for low SNR, the variant asynchronous by both at rate with versions manual (ab-m) and automatic (ab-a) are better than the variant asynchronous by positive at rate with versions manual (ap-m) and automatic (ap-a).

 ISBN: 978-1-61208-231-8

Fig. 13 shows the jitter-SNR curves for the prefilter bandwidth B2=2.tx with the four synchronizers (ab-m, ab-a, ap-m, ap-a).

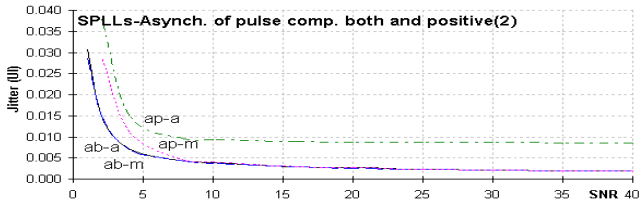


Figure 13. Jitter-SNR curves of B2+4synchronizers (ab-m, ab-a, ap-m, ap-a)

For prefilter B2=2.tx, we verify that, it becomes the jitter-SNR curves more similar between themselves. For high SNR, it degrades slightly the jitter-SNR curves. However, for low SNR it benefits significantly the jitter - SNR curves.

Fig. 14 shows the jitter-SNR curves for the prefilter bandwidth B3=1.tx with the four synchronizers (ab-m, ab-a, ap-m, ap-a).

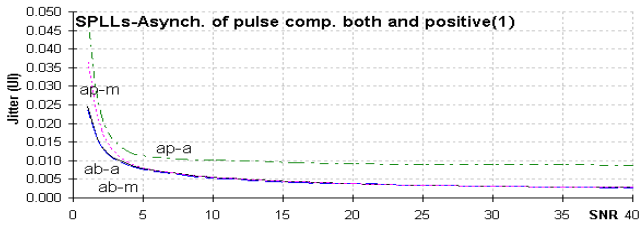


Figure 14. Jitter-SNR curves of B3+4synchronizers (ab-m, ab-a, ap-m, ap-a)

For prefilter B3=1.tx, we verify that, it becomes the jitter-SNR curves still more similar between themselves. For high SNR, it harms more the jitter-SNR curves. However, for low SNR, it benefits less the jitter-SNR curves.

VI. CONCLUSION AND FUTURE WORK

We studied three prefilter bandwidths (B1=∞, B2=2.tx, B3=1.tx) with four synchronizers, one variant asynchronous by both transitions at rate with versions manual (ab-m) and automatic (ab-a) and other variant asynchronous by positive at rate with versions manual (ap-m) and automatic (ap-a). Then, we measured their jitter - SNR curves.

We observed that, in general, the output jitter curves decreases gradually with the input SNR increasing.

For prefilter B1=∞ (greater), we verified that, for high SNR, the four synchronizers jitter curves tend to be similar, this is comprehensible since all the synchronizers are digital and have similar noise margin. However, for low SNR, the variant asynchronous by both at rate with its versions manual (ab-m) and automatic (ab-a) is better than the variant asynchronous by positive at rate with its versions manual (ap-m) and automatic (ap-a), this is comprehensible because the variant by both transitions has more transitions (double) than the variant by positive transitions and then, the going time from the error state to the correct state is lesser.

For prefilter B_2=2.tx(medium), we verified that, it becomes the jitter-SNR curves more similar between themselves. For high SNR, it degrades slightly the jitter-snr curves. However, for low SNR, it benefits significantly the jitter-SNR curves.

For prefilter B3=1.tx (minor), we verify that, it becomes the jitter-SNR curves still more similar between themselves. For high SNR, it degrades more the jitter-SNR curves. Also, for low SNR, it benefits less the jitter-SNR curves.

So, the prefilter, for high SNR, distorts the signal what is prejudicial, for low SNR, attenuates noise what is beneficial.

In the future, we are planning to extend the present study to other types of synchronizers.

ACKNOWLEDGMENT

The authors are grateful to the program FCT (Foundation for sCience and Technology) / POCI2010.

REFERENCES

[1] Jean C. Imbeaux, “performance of the delay-line multiplier circuit for clock and carrier synchronization in Digital Satellite Communications”, IEEE Journal on Selected Areas in Communications pp. 82-95 Jan. 1983.

[2] Werner Rosenkranz, “Phase Locked Loops with limiter phase detectors in the presence of noise”, IEEE Transactions on Communications com-30 Nº10 pp. 2297-2304. Oct 1982.

[3] Hans H. Witte, “A Simple Clock Extraction Circuit Using a Self Sustaining Monostable Multivibrator Output Signal”, Electronics Letters, Vol.19, Is.21, pp. 897-898, Oct 1983.

[4] Charles R. Hogge, “A Self Correcting Clock Recovery Circuit”, IEEE Transactions on Electron Devices pp. 2704-2706 Dec 1985.

[5] Antonio D. Reis, Jose F. Rocha, Atilio S. Gameiro and Jose P. Carvalho “A New Technique to Measure the Jitter”, Proc. III Conf. on Telecommunications pp. 64-67 FFoz-PT 23-24 Apr 2001.

[6] Marvin K. Simon and William C. Lindsey, “Tracking Performance of Symbol Synchronizers for Manchester Coded Data”, IEEE Transactions on Communications Vol. com-2.5 Nº4, pp. 393-408, April 1977.

[7] Jeffrey B. Carruthers, D. D. Falconer, H. M. Sandler and L. Strawczynski, “Bit Synchronization in the Presence of Co-Channel Interference”, Proc. Conf. on Electrical and Computer Engineering pp. 4.1.1-4.1.7, Ottawa-CA 3-6 Sep. 1990.

[8] Johannes Huber and Weilin Liu “Data-Aided Synchronization of Coherent CPM-Receivers” IEEE Transactions on Communications Vol.40 Nº1, pp. 178-189, Jan. 1992.

[9] Antonio A. D’Amico, Aldo N. D’Andrea and Ruggero Reggianni, “Efficient Non-Data-Aided Carrier and Clock Recovery for Satellite DVB at Very Low SNR”, IEEE Jou. on Sattelite Areas in Comm. Vol.19 Nº12 pp. 2320-2330, Dec. 2001.

[10] Rostislav Dobkin, Ran Ginosar and Christos P. Sotiriou “Data Synchronization Issues in GALS SoCs”, Proc. 10th International Symposium on Asynchronous Circuits and Systems, pp. CD-Ed., Crete-Greece 19-23 Apr. 2004.

[11] N. Noels, H. Steendam and M. Moeneclaey, “Effectiveness Study of Code-Aided and Non-Code-Aided ML-Based Feedback Phase Synchronizers”, Proc. IEEE Intern. Conference on Communications (ICC’06) pp. 2946-2951, Istambul-TK, 11-15 Jun 2006.

[12] Antonio D. Reis, Jose F. Rocha, Atilio S. Gameiro and Jose P. Carvalho “Carrier Phase Lock Loop and Bit Phase Lock Loop”, Proc. IX Symposium on Enabling Optical Network and Sensors (SEONs) pp. CD-Edited, Aveiro-PT 1-1 July 2011.

 ISBN: 978-1-61208-231-8

Connecting Communities: Stories of Digital Adventures in a Third Sector Organization

Maria Burke
Salford Business School
University of Salford
Salford, UK
m.e.burke@salford.ac.uk

Abstract—This paper aims to give an overview of the implementation of read and write back Quick Read (QR Codes) and Radio Frequency Identification Data (RFID) technology to a third sector, charity organization. The context of the research project is the Internet of Things and this particular "snapshot" of the research created tagged items with a story or history of that item, which was then accessible to customers of the charity via relevant mobile apps. The paper discusses issues around knowledge and knowledge browsing, the background to the project, the initial pilot, the regional trial of ten weeks and the journey towards national roll out. Then, the paper considers aspects of knowledge recovery and concludes with thoughts about knowledge sharing.

Keywords-communities; third sector; QR codes.

I. INTRODUCTION

In order to attempt to "connect communities" we must first examine the medium we use to connect – and that is knowledge. In its simplest form, knowledge can be categorized, as explicit or tacit knowledge [1][2][3][4][5]. Members of a society produce knowledge via raw information. Society in general is organized into many different systems, (organizations), which are often controlled by technology. Within organizations knowledge systems utilize the available technology in order to undertake particular parts of the information management process – including careful planning of the way in which the information flows within the organization structure – resulting in overall improved control of the way in which the knowledge is managed. Due to the current, continuous nature of change in organizations today, it is critical that managers are able to respond and take prompt decisions. For example, new tagging technology can provide a means of improving business performance by offering a new way of browsing, recovering and sharing information such as an estate agent who is able to measure the performance of property adverts in local papers by offering clients the facility to "read additional information" via QR codes placed beside the property photo.

Another example is that of a recruitment manager who could dramatically affect the induction process by setting up a process for leaving "hidden" memories in the form of messages embedded in QR Codes, on items in offices, such as printers, keyboards; desks; walls, in order to speed the levels of efficiency and effectiveness, and again improve performance of the organization. The charity store manager may have the facility to personalize each donated gift through a technological facility where customers can listen to powerful memories associated with objects by "reading" the QR code. In these examples, knowledge that was tacit becomes available – available for others to browse; available as a form of recovered information (known but never written) and almost a type of mythological knowledge; and knowledge which is available to be shared using new forms of technology. All of these aspects are part of a broader discipline of knowledge management that can be defined as the process of locating, organizing, transferring and using the information and expertise within an organization. More formally, knowledge management can be defined as "the generation, representation, storage, transfer, transformation, application, embedding and protecting of organizational knowledge" [6] and this is the one that we consider best represents the work outlined in this paper. The old adage that the overall success of the organization, however, rests on one aspect, that of sharing information is still true, but with the onset of social media and newer more accessible technologies the ways of dealing with knowledge is changing. Now it is easy to share and indeed sometimes, difficult not to share.

What has become important and what will be discussed next is the ability to both "browse knowledge and to recover knowledge" and to show how tagging technologies can be applied in these areas.

II. KNOWLEDGE BROWSING

The confidence to browse suggests that an individual or organizations are comfortable in a context to afford them the time to survey products, services and perhaps people with whom they would like to connect. The act of browsing also suggests an open-minded disposition that is receptive to new modes of practice and interested less in finding answers to specific questions, but to understanding novel solutions, or even opportunities of which they were previously unaware.

 ISBN: 978-1-61208-231-8

What is important in this technological context is that aspect of browsing which we can define as "uncertainty". We will deal here with organizational uncertainty. Uncertainty can be viewed from two areas, that of "relational uncertainty" [7], where it is difficult for employees to predict the beliefs and behaviour of colleagues and that of "informational uncertainty" where the accuracy of the actual information is called into question- as addressed in the information seeking literature [8][9][10][11][12]. Both these areas are concerned with three issues. The first is the trepidation experienced by organizational members about levels of accuracy and quantity of information; the second issue is about both trusting the source of the information and a willingness to trust co -workers enough to share information whilst the third issue is about having sufficient relevant knowledge to make quality decisions. All of these issues are becoming clearer through the use and application of new forms of media and technology.

III. THE CASE STUDY – CONNECTING A COMMUNITY THROUGHT KNOWLEDGE

The project known as Tales of Things: Electronic Memories (TOTeM) aims to apply digital technology to the public at large, to business and to ensure that new kinds of technology are available and in a format which can be used by all sectors of society. The research is multi – institutional (Edinburgh, Salford, Brunel, UCL and Dundee Universities) and multi –disciplinary, and arises out of a research council Digital Economy Programme. During the project, a small pilot was launched working with a third sector charity store whereby a number of donated items were "tagged with QR codes which were embedded with the memory or history of that particular item. So, for example a teapot may be tagged with memories of families growing up and a variety of celebrations; a scarf may be tagged with memories of cold crisp winter days and so on. Audio facilities were located placed in the store, so that voices could be heard re-living the memory. In this way a very powerful atmosphere was created which enhanced the selling process and made the process of buying connected with the process of donating.

The short pilot was very successful with all the items sold and a high rise in revenue during that week. The value of the goods had been increased by the connection with memory. Later in the project, as the charity became familiar with the work, the team were involved in a larger study which involved ten charity shops over an initial period of twelve weeks. The team developed an App for use with iPhones that would encourage customers to try out the technology for themselves. The App could be downloaded to any Smartphone and used to read the QR Codes. Many items were tagged with QR Codes and placed on the shelf, ready for customers to read using mobile phones. The "stories" were interesting and varied – for example, the memory about a Party Dress (worn on a first date) to a pair of trainers (worn when running city Marathons) to memories of teapots and favourite cookbooks.)

A press launch took place and considerable interest was shown in the work. During the following ten weeks, 166 customers were interviewed about their experiences using the technology. The results were positive with most people enjoying the innovation and the novelty of accessing previously denied information. Donors' tended to spend less time leaving stories at drop off points, but buyers were keen on hearing the stories.

IV. KNOWLEDGE RECOVERY: THE CONTEXT OF MEMORY

Knowledge recovery is a new term and one that can be used to discover and recover information – to find out about memories and about identities of artifacts, to engage almost with history. This kind of knowledge is embedded personally in an individual experience and depends on other factors such as personal belief, perspective and the accepted value system, Gourlay [13] discovers that tacit knowledge has the identical phrase and defines it as practical know-how. It is informal rather than formal among professional groups including managers. What is particularly interesting is that new forms of digital technology are used to enhance this process. For example, the web site talesofthings.com that allows users to record a "tale" about any object and to upload to a database, is a form of both knowledge sharing and knowledge recovery. As individuals we are able to share with relative ease, however this becomes more problematic for us as we spend most of our lives dealing with or as part of organizations that operate within an ever-changing external environment. How then, can knowledge recovery both implicit and explicit be enhanced through digital technology? We may start to approach this problem by analyzing types of societies. This may be helpful as it allows us to consider the aspect of sharing information and the management of knowledge from quite different perspectives than technology and sociology. For example, Van der Ritja [14] was concerned with the two concepts of societies which displayed characteristics associated with individualism and collectism. These types of societies are important and provide means of charting differences in the concept of sharing [15][16].

V. KNOWLEDGE SHARING

Sharing generally happens within the context of an information system or a knowledge management system. For example, the work carried out in 2004, [17] concerned a virtual learning environment for French Physics teachers. This was an important study as it showed how the sharing of knowledge through the use of IT could be used to successfully "mediate" information, learning and understanding. Yet, the popularity and availability of social media sites has made "sharing" a much more social activity. Sharing in organizations only takes place where there is trust and where there is a shared feeling of ownership of goals. The reasons behind the tendency to share are based on the kind of interpersonal relations between co- workers inherent within the organization and the effects of social relationships

 ISBN: 978-1-61208-231-8

on organizational teams. Strengthening the social relationships between individuals in the team is crucial in motivating team members to share knowledge.

The current thinking in the research community about knowledge sharing within organizations is that barriers to knowledge sharing can be classified into individual barriers, organizational barriers and technology barriers. The UK has a rich array of examples where attention has been paid to knowledge management initiatives in order to set up major knowledge management systems, e.g. the Health Service and Banking sectors. Although these have not always been wholly successful, UK companies have taken up the ideas of knowledge management and have endeavored to identify and overcome barriers to sharing [18]. Of particular interest is the work [19], which investigated knowledge sharing capabilities and knowledge development needs in the context of East-West technology. However, in order for even the most basic KM system to work effectively, as we have seen, (above) there must be a sense of trust in the organization and this trust is crucial to the open sharing of information. Sharing only takes place where there is trust and where there is a shared feeling of ownership of goals. Within a business, this is often done through a framework of knowledge sharing networks. For example, Dyer and Nobeoka [20], on the Toyota's network can be seen as a purely classical way as having solved

"three fundamental dilemmas with regard to knowledge sharing by devising methods to (1) motivate members to participate and openly share valuable knowledge (while preventing undesirable spillovers to competitors), (2) prevent free riders, and (3) reduce the costs associated with finding and accessing different types of valuable knowledge. Toyota has done this by creating a strong network identity with rules for participation and entry into the network. Most importantly, production knowledge is viewed as the property of the network".

VI. CONCLUSION

There seems to be a high-degree of interest in the project and the responses have been mostly positive, but the user statistics suggest that this has not yet translated into "a story for every object". An Android application may have helped gather more stories and questionnaire responses, although iPhone users were the most prolific respondents to the questionnaire. The creation of an iPhone application for this trial can be justified by the results on Smartphone usage. The work is ongoing and evolving as both the technology changes and communities become less fragmented as knowledge is recovered and new knowledge is added, and ultimately memories are enriched.

The digital adventure of sharing, of connecting communities both locally and globally is ongoing, exciting and dynamic. The ability of technology to radically shift our perception of value is changing the life of communities towards more sustainable futures.

ACKNOWLEDGMENT

TOTeM (Tales of Things and Electronic Memory) is a collaborative research project and I acknowledge contributions from all the TOTeM Research Team - C. Speed, Edinburgh University; A. Karpovich, Brunel University; A Hudson Smith, University College London; S. O'Callaghan and Jon Rogers of Dundee University and all our research staff. TOTeM is funded through a grant from the Digital Economy Research Councils UK.

REFERENCES

[1] H.M.Ali and N.H. Ahmad, "Knowledge management in Malaysian banks: A new paradigm," Journal of Knowledge Management Practice," vol 7,(3) 2006 pp.73-79 Retrieved: November, 2012 from http://www.tlanc.com/articl120.htm

[2] W. Zheng, "A Conceptualisation of the relationships between organisational culture and Knowledge management," Journal of Information and Knowledge Management, vol 4(2) 2005 pp.113-124.

[3] S.Song, "An internet knowledge sharing system." Journal of Computer Information Systems, Spring, 2002, pp. 25-30.

[4] S.Kim and H.Lee, "The impact of organizational context and information technology on employee knowledge-sharing capabilities", Public Administration Review. May/June, 2006, pp.370-385.

[5] M. H. Brent and S.A.Vitall, "Knowledge sharing in large IT organizations: a case study," VINE The Journal of Information and Knowledge Management Systems vol. 37 (4) 2007 pp. 421-439.

[6] U. Schultze and D. Leidner, "Studying KM in IS research: discourses and theoretical assumptions," MIS Quarterly vol. 26 (3) 2002, pp. 213-242.

[7] C. R. Berger, Beyond initial interaction: uncertainty,understanding and the development of interpersonal relationships, pp. 122-145 in H. Giles and R. St Clair, (Eds), Language and social psychology, Oxford: Blackwell, 1975.

[8] M. Burke, "Cultural issues, organizational hierarchy and information fulfilment: an exploration of relationships," Library Review, vol. 56 (8) 2007, pp. 236-245.

[9] M. Burke, "Philosophical and theoretical perspectives of organization structures as information processing systems," Journal of Documentation vol.59 (2) 2003, pp.131-142.

[10] M. Burke, "Achieving information fulfilment in the networked society, Part 1: Introducing new concepts," New Library World, vol. 107 (9/10) 2006, pp. 21-26.

[11] C.Choo, "Environmental scanning as information seeking and organizational learning," Information Research, vol. 7 (1) 2001, pp.35-39 Retrieved: November, 2012 from http://informationr.net/ir/7-1/paper112.html

 ISBN: 978-1-61208-231-8

[12] C. Kulthau, "A Principle of uncertainty for information seeking," Journal of Documentation, vol. 49 (4) 1993, pp.39-55.

[13] S. Gourlay, "Knowledge management and HRD", Human Resource Development International, vol. 4 (1) 2001, pp. 27-46.

[14] P. Van der Rijta, Precious knowledge: virtualness and the willingness to share knowledge in organisational teams. Amsterdam: University van Amsterdam Press, 2007.

[15] C. Chen, "How can cooperation be fostered? The cultural effects of individualism-collectivism," Academy of Management Review, vol. 23, (2) 1998, pp. 285- 304.

[16] G. Hofstede and G. J. Hofstede, Cultures and organizations. software of the mind. London: McGraw Hill, 2005.

[17] M. Kalogiannakis, "A virtual learning environment for the French physics teachers," Education and Information Technologies, vol. 9, (4) 2004, pp. 345-353.

[18] K.Y.Wong and E. Aspinwall, "An empirical study of the important factors for knowledge management adoption in the SME sector.," Journal of Knowledge Management, vol. 9, (3) 2005, pp. 64-82.

[19] T. Elenurm, "Entrepreneurial knowledge sharing about business opportunities in virtual networks", Proc. 8th European Conference on Knowledge Management, (ECKM 07) May, 2007, pp.285-290.

[20] J.H. Dyer and K. Nobeoka, (2000). "Creating and managing a high-performance knowledge-sharing network: the Toyota case," Strategic Management Journal, vol. 21, 2000, pp.345–349.

 ISBN: 978-1-61208-231-8

Distance-Adaptive Routing and Spectrum Assignment of Deadline-Driven Requests in Reconfigurable Elastic Optical Networks

Jared Morell and Gokhan Sahin
Electrical and Computer Engineering Department
Miami University
Oxford, OH, U.S.A.
e-mail: morellja@muohio.edu, sahing@muohio.edu

***Abstract*—Spectrum-sliced elastic optical networks, enabled by technological advances such as CO-OFDM, bandwidth-variable transponders, bandwidth-variable optical cross-connects, and optical multi-level modulation, provide a means to divide the spectrum on a finer granularity than WDM and to slice-off just the adequate amount for each connection. It is envisioned that these networks will carry various types of traffic with different service level guarantees, including deadline-driven requests (DDRs) that require the data to be transferred by a given deadline without imposing a specific constant bandwidth requirement. As a result, DDRs can be provisioned with variable transmission rates between their arrival times and deadlines. We consider the DDR-provisioning problem in a reconfigurable elastic optical network that supports such bandwidth readjustments through minimal reconfiguration in the network, and develop a distance-adaptive routing, spectrum assignment, and reconfiguration algorithm for this purpose. Our results show major improvement in performance due to bandwidth reallocation of DDRs in elastic networks over a range of reconfiguration delay parameters.**

Keywords - deadline-driven traffic; elastic optical network; optical OFDM; routing modulation level and spectrum assignment; network reconfiguration.

I. INTRODUCTION

In high capacity optical transport networks, wavelength division multiplexing (WDM) has allowed for the spectrum division of channels into wavelengths of smaller bandwidth on a fixed-grid. Its rigidity and coarse granularity pose drawbacks, however, for clients and service providers. These wavelength-routed networks require full allocation of a wavelength even when the transmission across the channel is not sufficient to fill the wavelength's capacity. Similarly, if a connection needs more than a wavelength's worth of spectrum, it must occupy at least another wavelength to be accepted. This results in poor spectrum utilization.

Over the past few years, a substantial amount of effort has been put forth in designing and developing elastic optical networks based on spectrum slicing [1]. This network type has become known as spectrum-sliced elastic optical path network, or SLICE. Spectrum slicing is a means to divide the spectrum on smaller levels and "slice-off" just the amount necessary for an end-to-end connection request. Technological advances such as the bandwidth-variable (BV) optical cross-connect (OXC), BV transponder, optical multilevel modulation, and optical orthogonal frequency-division multiplexing (OFDM) have enabled an optical fiber to be transformed into a much more manageable and effective data transport [1], [2]. Fig. 1 shows the spectrum usage difference in WDM and OFDM networks.

In optical OFDM networks, data is taken and spread over the necessary number of overlapping, low data rate subcarriers. The subcarriers are able to overlap within a connection and be fully recovered at the receiver due to their orthogonal nature. Being able to pack the subcarriers into a much smaller area than would be possible with WDM enhances the spectrum utilization greatly [3].

There are a number of different traffic types that optical networks support, e.g., best-effort and minimum bandwidth that require various quality-of-service guarantees. An emerging class of applications that need on-demand and flexible bandwidth allocation are deadline-driven applications [4]. As the name suggests, these are applications that require data be transferred by a given deadline. Because these applications do not require a strict, specified bandwidth, variable transmission rates can be used to accommodate the requests. Traffic such as this arises in such cases as eScience and grid-computing [5]. Because these fields utilize a distributed network of computers to perform a task, various parts are needed by certain times for everything to run smoothly. They therefore could benefit from deadline-aware service. Other systems that do not need immediate updates could make use of a deadline-driven service as well.

In this paper, we address the issue of routing, modulating, and dynamically allocating spectrum to deadline-driven requests (DDR) in reconfigurable elastic optical networks. The capability of elastic optical networks to dynamically adjust the spectrum allocated to connections makes them a suitable candidate for carrying DDRs due to their flexible bandwidth requirement. Although various aspects of routing and spectrum

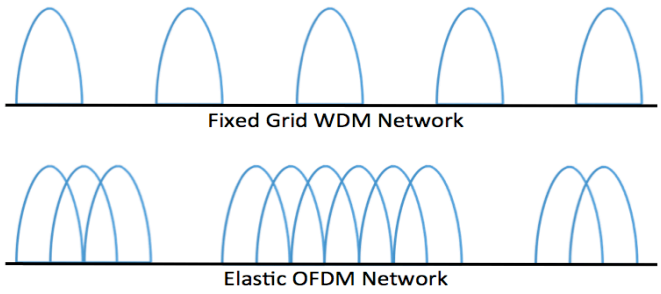


Figure 1. Comparing the spectrum of a WDM network with its fixed grid and that of an OFDM network with overlapping subcarriers.

 ISBN: 978-1-61208-231-8

assignment in elastic optical networks have been considered in recent work (see for instance [1-3, 6-8, 10]), we are not aware of prior research that addresses deadline-driven traffic in these networks. The problem that we consider is also different from earlier DDR work in WDM networks [4] due to the fundamental architectural differences between WDM-based and elastic optical networks. We explicitly consider various aspects of the problem that are specific to elastic optical networks, such as the need to allocate a contiguous band of subcarriers to a connection; the ability to choose a distance-adaptive modulation format for each sub-carrier, and the delay associated with reconfiguring the BV transponders and the BV OXCs in order to adjust the rates of an existing connection.

The rest of the paper is organized as follows. Section II formally presents the problem we are concerned with and the model we will be using. In Section III, we describe the method by which we accomplish the issue. Section IV delivers the results of our simulation. Finally, Section V concludes the paper and notes possible future work.

II. Problem Definition and Model

Establishing a connection in an OFDM-based network is substantially different from that in WDM networks. What was a wavelength continuity concern between links in a WDM network becomes an issue of subcarrier continuity in an OFDM network. In addition, in order to make use of the orthogonality of the subcarriers and maintain other architecturally desirable characteristics, they should be assigned in a contiguous manner within the link. Subcarriers from different connections should never overlap on a link. Fig. 2(a) illustrates this.

Each OFDM subcarrier can be modulated using, e.g., binary phase-shift keying (BPSK, 1 bit per symbol), quadrature phase-shift keying (QPSK, 2 bits per symbol), quadrature amplitude modulation (8QAM, 3 bits per symbol), and so on, to determine the data rate that each subcarrier can deliver. It is desirable to select the highest modulation level while still maintaining acceptable quality of transmission.

Additionally, because DDRs are allowed flexible bandwidth, spectrum allocation is not restricted to its availability at the time of arrival. Instead, reallocation may occur between the time of arrival and the deadline. Decreasing the bandwidth of an ongoing connection to accommodate an incoming request was first proposed in [4] for use in WDM networks. In this paper we will expand upon their 'Changing-Rates' method and apply it to an elastic network model. In our model, transmission of data can resume only after a delay following the bandwidth adjustment of an existing connection in order to accommodate the necessary reconfigurations, whereas an instantaneous bandwidth adjustment was assumed in [4].

The model that we are using for the elastic spectrum is a common one used for optical OFDM networks [2], [6], [7], [8]. Rather than looking at the spectrum as an open resource where subcarriers can be placed at any frequency, it can be thought of as divided into frequency slots, of width, F GHz, able to transmit at capacity

$$T = MC, \tag{1}$$

where T is in Gbps, M is the modulation multiplier, equal to 1 for BPSK modulation, 2 for QPSK modulation, etc., and C is the base capacity of a subcarrier using BPSK modulation (in Gbps). Fig. 2 (b) shows how the frequency slots relate to the actual overlapping subcarriers on the spectrum. To avoid interference, a guardband, G, of a certain number of frequency slots is required between connections.

Once a request arrives at the network, we are tasked with finding a path from its source to destination node with at least enough contiguous subcarriers to transfer its total file size by the deadline. If such a path is not immediately available, we attempt to perform a reallocation algorithm which would adjust the bandwidth of the smallest number of ongoing connections to make room for the incoming request. The next section describes the algorithm by which this is done.

III. Provisioning Deadline-Driven Requests in Reconfigurable Elastic Optical Networks

A request, R, arrives at the network and is defined by the following parameters

$$R = (\sigma, \delta, S, D), \tag{2}$$

where σ is the source node, δ is the destination node, S is the size of the file to be transferred (Gb), and D is the deadline of the request. Requests arrive uniformly across the network with arrival rate, λ requests per second. Upon arrival, the K shortest paths are computed for the request, without regards to spectrum availability at the time. We then iterate over the K shortest paths, searching for a void of frequency slots. To do so, we must first characterize each link in the network by a subcarrier availability vector, of size *maxSub*, equal to the number of subcarriers on a link [2].

$$u_l = [u_{li}] = (u_{l1}, u_{l2}, \ldots, u_{lmaxSub}). \tag{3}$$

The variable l designates the particular link. The value of each u_{li} is equal to 1 if that subcarrier is available on that link, and 0 if it is not. It is possible to compute the path, p, subcarrier availability vector, U_p, by using the Boolean AND operation over all $l \in p$. This is what is used to first search for a sequence of unoccupied subcarriers on each path. Applying the subcarrier contiguity constraint, we search for the smallest spectrum void (free sequence of frequency slots) that can occupy the incoming request.

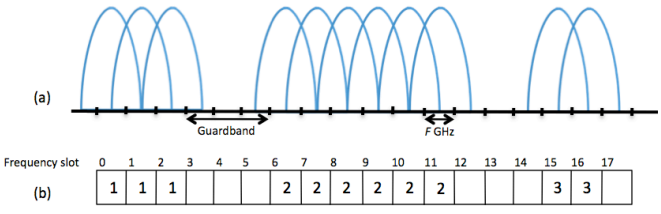


Figure 2. Relationship between the overlapping subcarriers (a) of several connections and an equivalent frequency slot model (b).

 ISBN: 978-1-61208-231-8

To figure out how many frequency slots are necessary, we must also determine the highest modulation level that is acceptable to apply to each subcarrier. It is a common simplifying assumption for such studies that the sole quality of transmission factor is the distance traversed [2]. For distances up to 6000 km, BPSK modulation can be used. For every halving of the transmission distance, the signal quality improves enough to increase the modulation level by 1 bit per symbol [9]. Thus, each path has its own M_p modulation level multiplier, and as a result, its own frequency slot transmission capacity, T_p, and necessary number of subcarriers used to transmit data,

$$X_{p\_min} = \text{ceil}[\, S / (\,(D - A)T_p\,)\,], \tag{4}$$

where A is the arrival time of the request. However, not only is it necessary to find X_{p_min}, but there must be a guardband between neighboring connections. Therefore, the total minimum number of frequency slots required by incoming request, R, is

$$Y_{p\_min} = X_{p\_min} + G. \tag{5}$$

Iterating from the shortest to the longest of the K paths, we search for the smallest void, *minVoid*, of frequency slots in U_p that is greater than or equal to Y_{p_min}. If found on p, we are able to accommodate the incoming request. We then set the total frequency slots occupied by this request, $Y_R = minVoid$, note its starting index, compute its departure time,

$$dep_R = S / (\,(Y_R - G)T_p\,) + t, \tag{6}$$

with t being the current time in the system, update the u_l vectors, and add the connection to the list of those currently in the network. If no void large enough was found on any path, we go to the reallocation phase.

In reallocation, we attempt to shrink the bandwidth of ongoing connections in order to accommodate the incoming request, while still being able to complete data transfer by their deadlines. We attempt reallocation with the shortest path first, and then move to each successive path from there. While attempting reallocation, we are always looking for a section of frequency slots that will affect the smallest number of ongoing connections.

For path, p, we first determine a new X_{p_min} and Y_{p_min}. These are determined by including a time penalty in the calculation in Equation 4, as follows.

$$X_{p\_min} = \text{ceil}[\, S / (\,(D - A - tPen)T_p\,)\,], \tag{7}$$

where *tPen* is a constant penalty time to account for reconfiguration. Y_{p_min} is computed in the same way as in Equation 5. We then locate any connections that interfere on at least one link of the incoming request's path, and add them to a list, *List*. These are the connections that will be checked for reallocation at each step in the process.

We iterate over U_p, starting from index 0, up to $maxSub - 1$, examining each frequency slot, s, and the possibility of reallocating connections around it. Void sizes are kept track of in the same manner as the original search for free frequency slots. If the frequency slot we are examining is:

A. The start of a new void ($U_{ps} = 1$ and $U_{ps-1} = 0$)

Simply set the void counter, *void*, to 1.

B. Still in the void ($U_{ps} = 1$ and $U_{ps-1} = 1$)

Increase *void*.

If $s = maxSub - 1$, we iterate over *List*, checking what connections lie in the range of $(s - Y_{p\_min}, s)$. Those that do would need to be reallocated by enough subcarriers so that they no longer are in that range. If each connection in *List* is either able to be reallocated or does not fall in that range of subcarriers, we have arrived at a possible reallocation scenario and make note of the connections that need adjusted and by how much.

C. Occupied ($U_{ps} = 0$)

If:

1) This is the first frequency slot ($s = 0$)

Perform a similar attempt to reallocate as in (*B*.), but check in the range, $[0, Y_{p\_min})$.

2) This is the end of a void ($U_{ps-1} = 1$)

Iterate over a block of frequency slots encompassing the void in an attempt to reallocate connections within that block. The block is of size Y_{p_min}, and is initially placed with its starting index at $s - Y_{p\_min}$, and its last index at $s - 1$. Within that block, connections are attempted to be reallocated in a similar means as above. Then the block is moved forward one frequency slot and the process starts over. This continues until the block's last index reaches $s + Y_{p\_min} - void$.

3) Otherwise

Attempt to reallocate connections as done in (*B*.), but in the range, $[s, s + Y_{p\_min})$.

Once the frequency slot iteration has completed, we check if any possible connection reallocations were found. If they were, the section with the minimum number of connections being affected was selected. From there, those connections would be reduced and their parameters changed as follows,

$$S_R = S_R - (Y_R - G)T_p\,(t - A_R), \tag{8}$$

$$A_R = A_R + tPen, \tag{9}$$

$$Y_R = Y_R - red, \tag{10}$$

$$dep_R = S / (\,(Y_R - G)T_p\,) + A_R, \tag{11}$$

where *red* is the amount by which that connection needs reduced. S_R now becomes the file size left to transfer, and A_R becomes the time at which connection resumes. Also, if any connections were reduced from their front, their initial indices would need shifted as well. The u_l vectors are updated as well, indicating free slots where the connections were reduced.

Now the incoming request can be added to the network where other connections have made space available. Its

 ISBN: 978-1-61208-231-8

selected path and starting index are noted, departure time set, as in Equation 11, and Y_R set to Y_{p_min}. The u_l vectors are once again adjusted to account for the incoming connection.

If it is not possible to reallocate connections on any path, in order to make room for the incoming connection, the request is blocked.

IV. RESULTS

Two different networks were used for this simulation. They were the US NSFNET topology, consisting of 14 nodes and 21 links, and the pan-European COST 266 network, made up of 28 nodes and 41 links [10]. Using F = 5 GHz, C = 2.5 Gbps, G = 2, *tPen* = 0.05 s, *maxSub* = 600, we evaluated the performance of our algorithm based on the fraction of blocked requests, while varying λ, D and S. On each simulation run, we held a different value of λ constant for use on all nodes in the network and uniformly distributed the values of D and S between set limits. Fig. 3 shows the algorithm's performance on both optical networks when compared to the scenario when no reallocation is considered. Here, the ranges of D and S are 3 – 100 s and 30 – 500 GB, respectively.

We also examined the case of having similar file sizes, but tighter deadlines, in the range of 2 – 5 s. This can be seen in Fig. 4.

In both cases, it is shown that the reallocation algorithm allows the network to service a far greater percentage of connection requests than if no reallocation were considered. There is a 20 – 35% difference in blocking probability between using and not using reallocation, over the simulated arrival rates for the relaxed deadline scenario and a 16 – 31% difference for the tight deadline case. This clearly demonstrates better spectrum utilization, as more connections can be placed into equivalent spectrum space.

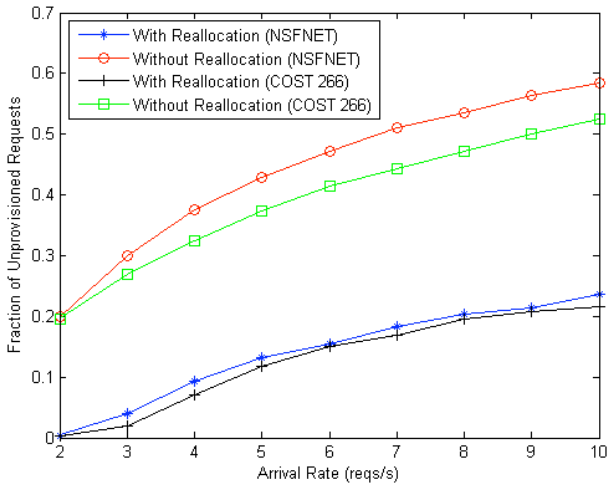


Figure 3. Comparing the routing and spectrum assignment algorithm with and without the reallocation phase

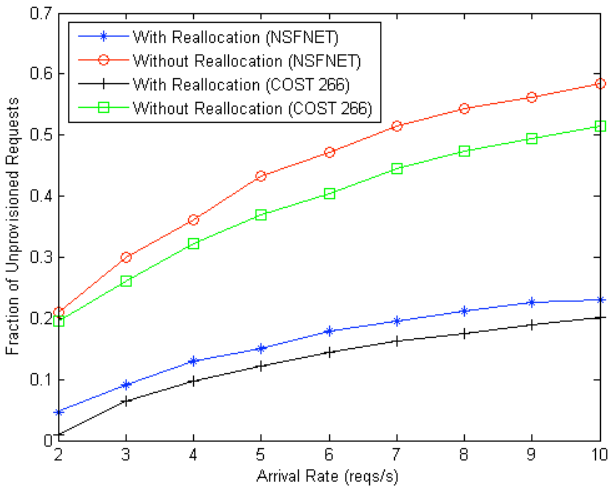


Figure 4. Comparing the routing and spectrum assignment algorithm for tight deadlines with and without the reallocation phase

V. CONCLUSION AND FUTURE WORK

We have developed an algorithm that allows a reconfigurable elastic optical network to accommodate deadline-driven requests with possibility of changing data rates. The method for reallocation allows the network to reconfigure ongoing connections in order to make room for a new request. In the future, it would be worth looking into reallocating and/or shifting connections at times other than request arrivals. Also, the means by which a void is chosen could be altered and different network and traffic scenarios could be analyzed.

REFERENCES

[1] B. Kozicki, H. Takara, Y. Tsukishima, T. Yoshimatsu, K. Yonenaga, and M. Jinno, "Experimental demonstration of spectrum-sliced elastic optical path network (SLICE)," Optics Express, vol. 18, no. 2, pp. 22105-22118, October 2010.

[2] K. Christodoulopoulos, I. Tomkos, and E. A. Varvarigos, "Elastic bandwidth allocation in flexible OFDM-based optical networks," Journal of Lightwave Technology, vol. 29, no. 9, pp. 1354-1366, May 2011.

[3] J. L. Vizcaino, Y. Ye, and I. T. Monroy, "Energy efficiency analysis for flexible-grid OFDM-based optical networks," Computer Networks, vol. 56, no. 10, pp. 2400-2419, July 2012.

[4] D. Andrei, M. Tornatore, M. Batayneh, C. U. Martel, and B. Mukherjee, "Provisioning of deadline-driven requests with flexible transmission rates in WDM mesh networks," IEEE/ACM Transactions on Networking, vol. 18, no. 2, pp. 353-365, April 2010.

[5] I. Foster, M. Fidler, A. Roy, V. Sander, and L. Winkler, "End-to-end quality of service for high-end applications," Computer Communications, vol. 27, no. 14, pp. 1375-1388, September 2004.

[6] M. Jinno et al, "Distance-adaptive spectrum resource allocation in spectrum-sliced elastic optical path network," IEEE Communications Magazine, vol. 48, no. 9, pp. 138-145, August 2010.

[7] G. Zhang, M. De Leenheer, and B. Mukherjee, "Optical grooming in OFDM-based elastic optical networks," Proc. OFC/NFOEC, Paper OTh1A, March 2012.

 ISBN: 978-1-61208-231-8

[8] T. Takagi et al, "Dynamic routing and frequency slot assignment for elastic optical path networks that adopt distance adaptive modulation," Proc. OFC/NFOEC, Paper OTuI, March 2011.

[9] A. Bocoi, M. Schuster, F. Rambach, M. Kiese, C. Bunge, and B. Spinnler, "Reach-dependent capacity in optical networks enabled by OFDM," Proc. OFC/NFOEC, Paper OMQ4, March 2009.

[10] A. Betker et al, "Reference transport network scenarios," MultiTeraNet Report, July 2003, retrieved: September, 2012, http://wall.ikr.uni-stuttgart.de/en/Content/Publications/Archive/Ko_ITGPhotNetze04_36322.pdf.

 ISBN: 978-1-61208-231-8

QoS Aware Multi-homing in Integrated 3GPP and non-3GPP Future Networks

Umar Toseef*†, Yasir Zaki†, Liang Zhao†, Andreas Timm-Giel* and Carmelita Görg†
*ComNets, Hamburg University of Technology, Hamburg, Germany
Email: {umar.toseef, timm-giel}@tuhh.de
†TZI ComNets, University of Bremen, Bremen, Germany
Email: {yzaki, zhaol, cg}@comnets.uni-bremen.de

***Abstract*—In future networks, collaboration of heterogeneous wireless access technologies is inevitable. 3GPP has already standardized the interconnection of non-3GPP access technologies with the exiting 3GPP access networks. This enables users to make seamless vertical handovers between available access networks. However, the question still remains whether the non-3GPP access technologies can deliver the Quality of Service (QoS) demands of user applications? Within the context of the Open Connectivity Services (OConS) of the SAIL European project, this work investigates the effects of the integration of two network types on user Quality of Experience (QoE). In order to accomplish QoS guaranteed service from non-3GPP access technologies, this paper proposes a novel resource management algorithm. With the help of simulation results it is proved that network operators can get significant performance boost for their networks when the proposed scheme is deployed in an environment with heterogeneous access networks.**

Keywords: ***LTE and WLAN interworking, Efficient resource allocation, User QoE optimization, Multihoming in wireless heterogeneous networks***

I. INTRODUCTION

The EU-funded research project SAIL (Scalable & Adaptive Internet Solutions) research the design of the Networks of the Future, investigating new architecture for the future internet. The SAIL project is part of the European Commission's 7th Framework Program [1]. 24 operators, vendors and research institution are working together since 2010 on the research and development of novel networking technologies using proof-of-concept prototypes to lead the way from current networks to the Network of the Future [2]. The work of this paper falls within the solutions that the OConS work package is providing. The work ranges from concepts of OconS architecutre framework and Multi-P transmissions in LTE systems. The OConS approach is working on the proposal of an open and flexible architectural framework to handle the connectivity of networks. To fulfill the requirements and to keep the flexibility and openness of OConS, a component-based architecture frame-work is proposed, in 3 steps: (1) information collection; (2) decision making; (3) decision enforcement. These steps are handled by three functional entities:

- Information Management Entity (IE) is in charge of gathering the information required by decision making, e.g., link quality, power limitation, load and congestion of the networks. IE also pre-processes and filters the gathered information before it is delivered to the other entities.
- Decision Making Entity (DE) uses the information from IE to make the decision to fulfill some pre-defined metrics. For example, the final enforcements can be handover, load balancing and flow splitting. The goals of improving system performance can be maximizing the network throughput, balancing the load etc.
- Execution and Enforcement Entity (EE), finally, executes or performs the decision made by DE.

A. Motivation and Contributions

Nowadays, the end-user equipments are more and more powerful, and normally, have more than one interfaces which can connect to different wireless networks, e.g., 3G/4G mobile systems or wireless LAN (WLAN). On the other hand, the network resources are always scarce for supporting a huge number of users running different applications. The Multi-P algorithm, enables the interconnection of LTE and WLAN, so that end users can exploit all of the available wireless resources, meanwhile operators can also flexibly balance the traffic load among multiple access networks.

In this presented work, besides the general introduction to SAIL, OConS and Multi-P we put our focus on a simulation model realizing the Multi-P transmission of 3GPP LTE and WLAN. This involves development of simulation model according to 3GPP specifications, implementation of MIPv6 extensions to realize multi-homing and flow management techniques as well as the integration of user QoE evaluation tools in the simulator. With the help of intelligent resource management schemes we contribute towards network capacity improvements and user QoE enahancements.

The rest of this paper is organized as follows: Section II introduces the details of the OPNET[1] [20] simulation model for Multi-P. The traffic flow management strategies and the detailed mechanisms are described in Section III. For proof of concept, Section IV shows simulation results of different scenarios to reveal the advantages of our approach. At the end, Section V concludes this work and points out some possible points for our future works.

[1]OPNET Modeler®is a commercial network simulator which accelerates the R&D process for analyzing and designing communication networks, devices, protocols, and applications.

 ISBN: 978-1-61208-231-8

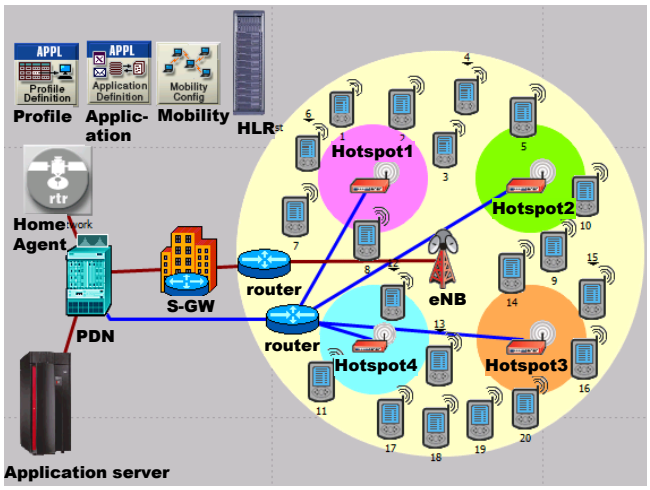


Fig. 1. Overview of the considered scenarios in OPNET. The large circular area represents the LTE access coverage. The small circular areas represent the coverage of WLAN access technology which overlaps LTE access coverage.

II. System Models

A. Applying Multi-P of OConS into interconnection of 3GPP LTE and WLAN

The goal of the presented work is to investigate the Interconnection (and cooperation) of 3GPP (e.g., LTE) and non-3GPP systems (e.g., Wireless Local Area Network (WLAN)) by means of the Multi-P transmission. The key part of this approach is the decision process: selection of interfaces of the UE and access alternatives (at the network side) that should be used for the transmission and how to manage the traffic flows.

From an architectural point of view as depicted in Fig. 1, the interconnection between 3GPP and non-3GPP (in our case we have chosen LTE and WLAN as case study) is possible at the Packet Data Network Gateway (PDN GW). Hence, it becomes a reasonable location for the DE of the network controlled Multi-P decision. For the LTE side, the IEs are located at the eNodeB (eNB) and the access gateway (aGW). For the WLAN side, the IE is located at the Wireless Access Point (WAP). UE also has IE and DE to gather the downlink information for the Multi-P decisions and to execute the Multi-P transmission.

B. OPNET Simulation Model

3GPP specified SAE [19] architecture allows a mobile user to roam between 3GPP and non-3GPP access technologies. In order to provide users with seamless mobility Proxy Mobile IPv6 (network based mobility) and Dual stack Mobile IPv6 (host based mobility) have been proposed [19]. We follow this proposal in the integration of 3GPP access technology (namely LTE) and trusted non-3GPP access technology (namely, legacy WLAN 802.11g), where host based mobility solution i.e., Dual stack Mobile IPv6 is considered. According to current 3GPP specification multi-homing is not supported. This implies that a user can either be associated to LTE network or WLAN network but cannot connect to both networks simultaneously. This work extends the 3GPP specified architecture to give users multi-homing capabilities. This is achieved by extending the implementation of MIPv6 to support multiple care-of address [14] and flow management functionality [12][13].

Fig. 1 shows an overview of the simulation network implemented in OPNET. All entities of SAE architecture which are necessary to carry out multi-homing scenario have been implemented. As per 3GPP proposal home agent (HA) function is located at PDN gateway. All users are considered to be out of home network during the complete simulation time. Remote server acts a correspondent node (CN) from where mobile users access application services like VoIP, Video and FTP. Users receive router advertisements from eNB and possibly from WLAN access point to configure care-of addresses. These care-of addresses are then registered with their HA through standard MIPv6 signaling. In this way all user traffic is tunneled from HA to the user.

It should be noted that our focus is only on the downlink access for LTE and WLAN. This implies that no uplink transmissions are performed for WLAN during the whole simulation time. Instead all uplink traffic (e.g., TCP ACK packets etc.) is transmitted by the user through LTE access link.

The original OPNET simulator does not adjust PHY data rate of WLAN users dynamically based on the received signal strength. This behavior has been modified based on literature survey [15] to bring it closer to the reality. As a result of this extension the user PHY data rate changes dynamically based on the received signal strength. However, the users are served by the access point only if their channel conditions are good enough allowing them to transmit at PHY data rate of 6Mbps or better. This is to avoid WLAN netwrok performance degradations due to users with low PHY data rate e.g., 1Mbps, 2Mbps etc.

OPNET provides no mechanism to evaluate voice call quality for wideband G.722.2 [17] codec. A procedure according to ITU-T recommendation has been introduced to evaluate voice call quality for simulation results as detailed in [18]. Furthermore, OPNET has also no support for realistic video traffic generation using any standard codec. Another extension has been made to generate realistic video call traffic according to MPEG-4 codec and evaluate the video call quality at the receiving end as proposed in [16].

III. Traffic Flow Management

A network operator can manage the traffic flow of a multi-homed user either by switching the complete traffic flow from one path to another or by splitting it into multiple sub-flows in a way that each path carries one sub-flow. These sub-flows are then aggregated at the destination to reconstruct the original traffic flow of the application. Though the option of splitting a traffic flow involves more sophisticate techniques, it provides greater flexibility in network load balancing. That is why in this work, flow management with flow splitting option is implemented and analyzed with the help of simulations.

 ISBN: 978-1-61208-231-8

A very basic question related to flow splitting option is: What should be an appropriate size of sub-flows (in bits/sec) transported to a multi-homed user over each path? In other words, how much traffic should be sent to user on each of the available access links? And a straightforward answer would be: each path or link should be loaded according to its bandwidth capacity. Moreover, when considering the flow splitting option one should also think how these sub-flows will be aggregated at the receiving end. In the following subsections, answers to these two questions are addressed.

A. Estimation of Link Capacity

1) WLAN Access Technology: Legacy WLAN (802.11 a/b/g) provides no QoS when scheduling user traffic. Essentially, there is only single queue in a WLAN access router where all incoming traffic is received and then transmitted over the air to the users in a "First Come First Serve" manner. That's why overall throughput of a hotspot and that of the users being served is highly variable based on number of active users in the system, their offered traffic load as well as their channel conditions. One way to estimate the throughput of a user is by knowing how much data have been sent to the user in a certain time window. However, this option has a serious drawback; it can only be used if there is already some data flowing to the user over WLAN link. Therefore, during time when a user has just attached to an access point and has not yet received any data over WLAN link, its potential bandwidth capacity over WLAN link cannot be estimated. Sending an arbitrary amount of data traffic on WLAN link without the knowledge of its capacity may lead to excessive queuing delays and buffer overflows at the WLAN access point.

This work proposes a novel way of scheduling available WLAN bandwidth resources in an efficient way which also provides an accurate estimation of user bandwidth capacity over its WLAN link. This approach needs following pieces of information to work i.e., number of active users attached to WLAN access point and their PHY data rate at a particular time instance. Once the number of active users associated to an access point N is known and they are assumed to be served in round robin manner, throughput of a user i denoted by $\lambda^{\mathrm{rr}}_{\mathrm{user}i}$ can be easily computed. Let's take t_i as the time required to transmit one complete IP packet of size p_i bits. The value of t_i can be computed based on user's current PHY data rate, packet size and MAC/PHY protocol overhead bits. Now that

$$\lambda^{\mathrm{rr}}_{\mathrm{user}i} = \frac{p_i}{\sum_{i=1}^{N} t_i}. \tag{1}$$

Similarly the access point throughput $\lambda^{\mathrm{rr}}_{\mathrm{AP}}$ is given by

$$\lambda^{\mathrm{rr}}_{\mathrm{AP}} = \frac{\sum_{i=1}^{N} p_i}{\sum_{i=1}^{N} t_i}, \tag{2}$$

The assumption that access point serves users in round robin manner can be realized by performing an intelligent flow splitting at HA. Actually HA is the entity where flow management function decides to which user's care-of address a packet will be forwarded. For all users who are being served by the same access point, their data traffic packets are sent towards the serving access point in the round robin manner i.e., one packet from first user, next packet from second user, and so on. Owning to the fact that no packet re-ordering takes place on the transport link from PDN-GW to the access point, all of these packets will be buffered in the FIFO queue of the access point in the sent order. In this way, when these packets are transmitted to the users it can be claimed that users are being served by the access point in round robin manner.

The round robin way of scheduling WLAN resources, however, does not make optimum use of the resources. This point can be elaborated with following example. Consider a single active user attached to a WLAN access point who is receiving a UDP flow comprised of fixed IP packet size of p bits. Assuming 54Mbps PHY data rate, the user experiences a throughput of $p/t_{54\mathrm{Mbps}}$ where $t_{54\mathrm{Mbps}}$ is the time to transmit one packet. As soon as another user with 6Mbps PHY data rate (who is also receiving a similar UDP flow) associates to the same access point, the overall throughput now amounts to $2p/(t_{54\mathrm{Mbps}} + t_{6\mathrm{Mbps}})$. Considering basic channel access mechanism of 802.11g $t_{6\mathrm{Mbps}} \simeq 5.6 \cdot t_{54\mathrm{Mbps}}$ which implies that joining of second user reduces the overall access point throughput by 70%. This is because round robin is a fair scheme which gives equal chance of medium access to all active users irrespective of their channel conditions.

One way to overcome this drawback is performing flow splitting in such a manner which gives users with medium access in proportion to their PHY data rate values. In other words, the users are given equal share of time slice and in this way the users with the higher PHY data rate can transmit more packet compared to the users with lower PHY data rate. This scheduling effect can be achieved in the above described example if 56 packets from first user and 10 packets from second user are sent to WLAN access point by flow management function residing at HA. This will enhance the overall system throughput by 196% compared to simple round robin scheme. However, this overall system performance gain comes at the cost of reduction in throughput of second user. Nevertheless, the proposed scheme is fair enough to give a user system throughput share in proportion to his channel condition while considerably improving the overall system throughput.

In order to compute the throughput of a system which follows above mentioned WLAN resource scheduling scheme, let's define r_i as the achievable data rate for a user who is the only active user in the system. This amounts to $r_i = p_i/t_i$, where t_i is the time taken by user i to transmit a packet of size p_i bits when transmitting with a certain PHY data rate. Now, the user i's fair share from throughput resources in proportion to his achievable data rate r_i is given by w_i such that $w_i = r_i/(\sum_{i=1}^{N} r_i)$. This way, the overall system throughput $\lambda^{\mathrm{ch}}_{\mathrm{AP}}$ will be computed as following

$$\lambda^{\mathrm{ch}}_{\mathrm{AP}} = \frac{\sum_{i=1}^{N} w_i \cdot p_i}{\sum_{i=1}^{N} w_i \cdot t_i} \tag{3}$$

 ISBN: 978-1-61208-231-8

and the throughput of user i is given by

$$\lambda_{\mathrm{user}_i}^{\mathrm{ch}} = \frac{w_i \cdot p_i}{\sum_{i=1}^{N} w_i \cdot t_i} \quad (4)$$

The above described method of scheduling WLAN bandwidth resources is just one of the possible ways. In general, any scheduling scheme can be imposed using flow management function at HA.

2) LTE Access Technology: In case of LTE, it is not simple to compute the bandwidth capacity available to a user. This is because its value depends on several factors, e.g., MAC scheduler type, channel conditions of all users, QoS requirements of traffic from all users, cell load level, etc. This problem can, however, be solved by introducing a throughput metering function between PDCP and RLC layers at eNodeB. This metering function reports the average throughput of the user data flowing from PDCP to RLC layer in downlink direction. The reported throughput value is then taken as LTE link capacity of that particular user. In addition to frequent user throughput reports, the metering function also provides occupancy level of user PDCP buffer at eNodeB. PDCP buffer occupancy actually reflects the tendency of increase or decrease in user throughput. For example, when user throughput reduces due to some reason (e.g., cell overload or bad channel conditions) the egress data rate from PDCP buffer becomes lower than the ingress data rate which in turn makes PDCP buffer occupancy to increase. The opposite is true, when user throughput increases. Owing to this fact, flow management function at HA tries to keep PDCP buffer occupancy at a certain target level. During the events of decrease in PDCP buffer occupancy more user traffic is sent to LTE link till the target buffer occupancy level is achieved and vice versa. The amount of target buffer occupancy is decided dynamically as explained later in this section.

B. Sub-flow Aggregation Function

In multi-path communication, packet may arrive out of order at the destination [7]. Real time applications usually deploy a play-out (or de-jitter) buffer, which is intended to get rid of jitter associated with packet delays. However, it can also perform packet reordering if packets arrive within time window equal to play-out buffer length. In this way, real time applications face no problems when receiving out of order packets in multi-path communication unless delay of all paths is less than play-out buffer length.

On the other hand, TCP based application are very sensitive to packet re-ordering. This is because an out-of-sequence packet leads TCP overestimate the congestion of the network, which results in a substantial degradation in application throughput and network performance [6]. A literature survey shows that there are several proposals to make TCP robust against packet re-ordering [8]-[11]. The analysis and implementation of these schemes in our simulator is currently not within the focus of this research work. Instead, we implement a simple TCP re-ordering buffer at user side, which is very similar in functionality to a play-out buffer. Simulation analysis shows that re-ordering buffer length must be set as less than TCP protocol time out value. In this work, re-ordering buffer length has been kept between 100ms to 500ms. TCP re-ordering buffer length τ_{tcp} is a key factor in deciding target PDCP buffer occupancy level μ_i of a user i.e.,

$$\mu_i = \lambda_i^{\mathrm{LTE}} \cdot \tau_{\mathrm{tcp}}, \quad (5)$$

where λ_i^{LTE} is the estimation of LTE link throughput of the user.

With the help of this strategy, LTE link delay is controlled not to exceed the TCP re-ordering buffer length, and hence, avoid unnecessary TCP time-outs.

TABLE I
SIMULATION CONFIGURATIONS

Parameter	Configurations
Total Number of PRBs	50 PRBs (10 MHz specturm)
Mobility model	Random Direction (RD) with 6 km/h
Number of users	5 VoIP, 3 HD video & 5 Skype video call, 7 FTP downlink users
LTE Channel model	Macroscopic pathloss model , Correlated Slow Fading [3]
LTE MAC Scheduler	TDS: Optimized Service Aware [4], FDS: Iterative RR approach
WLAN technology	802.11g, RTS-CTS enabled, coverage $\approx$ 100 m
VoIP traffic model	G.722.2 wideband codec, 23.05kbps data rate
Skype video model	MPEG-4 codec, 512kbps, 640x480 resolution, 30fps, play-out delay: 250 ms
HD video model	MPEG-4 codec, 1Mbps, 720x480 resolution, 30fps, play-out delay: 250 ms
FTP traffic model	FTP File size: constant 10 MByte continuous file uploads one after the other.
Simulation run time	10^3 seconds,13 seeds, 98% confidence interval

IV. SIMULATION SCENARIOS AND RESULTS

The target of this section is to highlight the gains that can be achieved by extending the 3GPP inter-working architecture to support the simultaneous use of the multi interfaces. That means the aggregation of several wireless interfaces, in order to enhance the system performance. In this section, two main scenarios are compared against each other, that is, the 3GPP default architecture, where multi-homing is not supported however user can perform seamless Handover (HO) to switch between the multiple wireless networks, and this will be referred to as "3GPP HO". Whereas, the second scenario is the novel proposal of this paper, to extend the 3GPP architecture into supporting the simultaneous use of wireless interface, this will be referred to as "Multi-P".

For each aforementioned scenario, two simulations setup are investigated. The first setup is composed of 20 users with mixed traffic of: Voice over IP (VoIP), File Transfer Protocol (FTP), video conference (i.e., Skype video call), and High Definition (HD) video streaming. The users move within one LTE eNodeB cell, and within this cell four wireless access points or hot-spots are present as shown in Fig. 1. The second setup is a special case where 5 FTP users are moving within the restricted coverage of a wireless access point where no LTE access is available. The motivation behind the later setup

 ISBN: 978-1-61208-231-8

is to show how the resource management function of "Multi-P" scenario outperforms the default "3GPP HO" case. The simulation configuration parameters are shown in Table I.

A. Mixed User Traffic

In this subsection, the mixed traffic setup investigations are discussed. As stated earlier, two different cases are compared against each other, these are: "3GPP HO" scenario and "Multi-P" scenario. The first scenario does not make simultaneous use of LTE and WLAN access technologies. In this case, all traffic takes its path to the user through LTE access which is available everywhere. However, when user enters the WLAN coverage its traffic is completely handed over to WLAN. It is worth mentioning here that in the "3GPP HO" scenario the users make vertical handover of hard nature, i.e., the user are disconnected completely from one network, and establish a new connection to the other one. Though MIPv6 keeps all IP layer connections alive through seamless handover, users might lose some buffered data on the previously connected network. On the other hand, the "Multi-P" scenario enables the users to use WLAN access when they are in its coverage while still keep the LTE connection alive and using it at the same time. As a result, a bandwidth aggregation process of both wireless links is achieved.

Fig. 2 shows the spider web graph of the average user delay values. A spider web graph is a visualization technique that can show multiple results in one graph, and is used to compare different scenarios. The graph in Fig. 2 has four different axes, each representing one performance metric, mainly VoIP, Skype video, HD video, and FTP file transfer end-to-end delay.

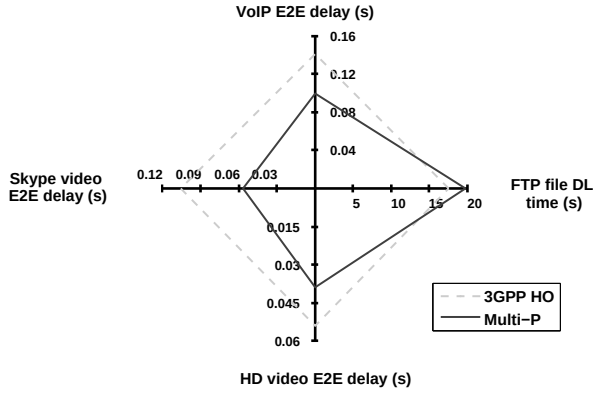


Fig. 2. End-to-end delay comparison spider web graph

Since all the axes represent delay, the algorithm producing the smaller shape has the best performance. In this case, it is clear that the "Multi-P" algorithm achieves the best results for the VoIP and videos traffic scenario. As for the FTP performance, it can be seen that the "3GPP HO" scenario has a slightly lower FTP file download time. However, the total number of 10MByte downloaded files is higher in the "Multi-P" scenario compared to the "3GPP HO" one (see Fig. 3). This is because in "3GPP HO" case some of the TCP connections abort due to excessive packet loss and sudden huge changes in TCP round trip time during the handover. In order to have performance evaluation comparison between the two scenarios, the Mean Opinion Score (MOS) values for the VoIP and the video traffics are shown in Fig. 4.

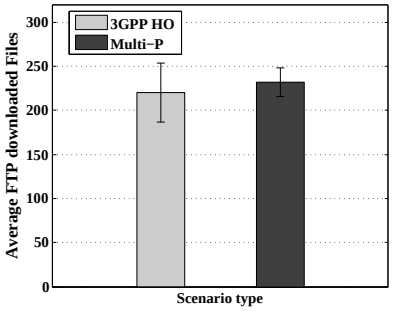


Fig. 3. Number of FTP downloaded files comparison

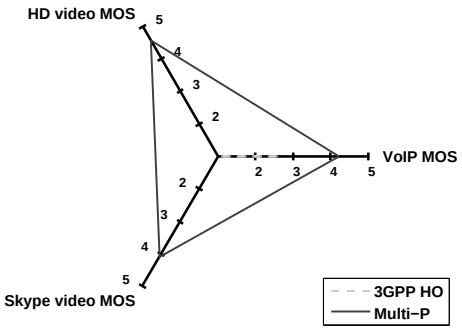


Fig. 4. VoIP and video MOS comparison

The results show that the "Multi-P" algorithm provides very good performance for the VoIP, as well as, for both video traffic types (Skype and HD). On the other hand, the "3GPP HO" scenario achieves very low MOS value for the VoIP users, the reason behind is, when VoIP users move from one access network to the other (from LTE to WLAN, and vice versa), the buffered data in the previous network is lost, and this affects the quality of the VoIP calls significantly as reflected in the MOS value. Furthermore, when VoIP and video traffic is transmitted over LTE, it is prioritized over FTP to achieve required QoS (i.e., throughput and delay). But when in "3GPP HO" scenario this traffic type is handed over to WLAN the required QoS cannot always be achieved due to lack of QoS differentiation support by 802.11g. Thanks to algorithms of "Multi-P" scenario which manages 802.11g resources in a way that not only the required QoS for real time traffic is met but also the optimum throughput performance of WLAN access point is accomplished. Moreover, in "Multi-P" scenario the loss of buffered data in network is avoided in the following manner. (i) LTE connection is always kept alive hence no buffered data is lost there. (ii) As far as WLAN link is concerned, the flow management function at HA sends user traffic on WLAN link only when user PHY data rate is 9Mbps or higher. This is because when a user has PHY data

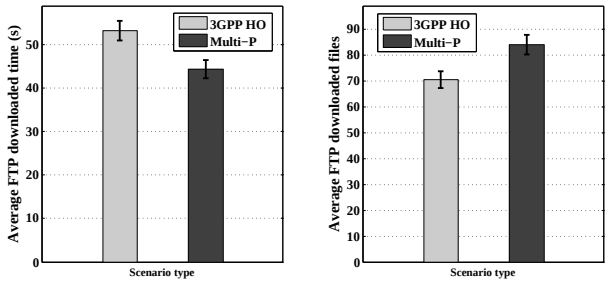
 ISBN: 978-1-61208-231-8

rate as 6Mbps it is a strong indication that loss of WLAN link is imminent. Hence, no new traffic data is sent on WLAN link for that user which gives him a chance to receive already buffered data from the access point before the loss of link.

It can be noticed that video users MOS values in "3GPP HO" scenario are not shown. The reason for that is the large packet loss rate due to two reasons: (i) buffered data loss at previously connected WLAN AP(ii) high end-to-end packet delay which makes play-out buffer discard the packets with delay greater than 250ms. Due this high packet loss rate, EvalVid tool [16] cannot evaluate the exact MOS value of the received video call implying that received video quality to too bad to be watchable. This limitation of EvalVid has already been discussed by the authors of the tool on their website.

B. FTP User Traffic

In this subsection, a special setup is investigated in order to highlight the advantages of using WLAN resource management algorithm discussed in Section III-A1. The scenario comprises of 5 FTP users, all moving within the coverage of the wireless access point without having LTE access. In both scenarios, the FTP users download constant 10MByte file size one after the other. Fig. 5(a) shows the average FTP file download time for both scenarios.



(a) Average file download time (b) Average downloaded files count

Fig. 5. FTP download performance

It can be seen, that the "Multi-P" scenario achieves a lower FTP file download time compared to the other scenario where no management of WLAN resources is performed. Moreover, the users in "Multi-P" scenario manage to download more files than in "3GPP HO" scenario. This shows that "Multi-P" scenario's algorithm of WLAN resource management does its job in optimum resource utilization to increase overall network throughput as explained in Section III-A1.

V. Conclusion

3GPP SAE architecture specifies how non-3GPP access technologies can be integrated in 3GPP networks and a seamless handover between these access technologies can be performed. This work proposed an extension to the specifications to allow a user benefit from all available access technologies by connecting to them simultaneously. The legacy WLAN does not provide QoS guarantee, and therefore not suitable for realtime interactive applications. However, through the use of suggested algorithms for resource management and accurate bandwidth capacity estimation WLAN bandwidth resources can be utilized for multi-homed users running QoS sensitive applications. In order to validate the proposed algorithm and procedures, an implementation of integrated network of LTE and legacy WLAN access technologies in OPNET simulator has been carried out. The simulation results provide proof of the concept where proposed scheme succeeds not only in providing QoS aware service to multi-homed users, but also optimizing the network bandwidth resource utilization. By outperforming the current 3GPP proposal, the new scheme assures a win-win situation for network operators as well as for users in future wireless networks.

VI. Acknowledgment

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7) under grant agreement no. 257448.

References

[1] SAIL project website: http://www.sail-project.eu/, acessed in Sept. 2012
[2] SAIL consortium, D.A.5: Exploitation and dissemination plan, 2010
[3] 3GPP Technical Report TS 25.814, Physical layer aspects for E-UTRA, 3rd Generation Partnership Project, v.7.1.0, Sept. 2006
[4] Y. Zaki, T. Weerawardane, C. Görg and A. Timm-Giel, Multi-QoS-Aware Fair Scheduling for LTE, Vehicular Technology Conference, 2011
[5] N. Zahariev, Y. Zaki, T. Weerawardane, C. Görg, and A. Timm-Giel. Optimized service aware lte mac scheduler with comparison against other well known schedulers. In 10th International Conference on Wired/Wireless Internet Communications, WWIC 2012, June 2012
[6] M. Laor and L. Gendel, The Effect of Packet Reordering in a Backbone Link on Application Throughput, IEEE Network, vol. 16, no. 5, pp. 28-36, Sept./Oct. 2002
[7] Ethan Blanton, Mark Allman. On Making TCP More Robust to Packet Reordering. ACM Computer Communication Review, 2002
[8] R. Ludwig and R. Katz. The Eifel algorithm: Making TCP robust against spurious retransmissions. ACM Computer Communication Review, 2000
[9] S. Floyd, J. Mahdavi, M. Mathis, and M. Podolsky. An extension to the selective acknowledgement (SACK) option for TCP. RFC 2883, 2000
[10] F. Wang and Y. Zhang. Improving TCP performance over mobile ad-hoc networks with out-of-order detection and response. In Proc. of the ACM MOBIHOC, 2002
[11] Stephan Bohacek, Joao P. Hespanha, Junsoo Lee, Chansook Lim, Katia Obraczka, TCP-PR: TCP for Persistent Packet Reordering, Proceedings of the 23rd International Conference on Distributed Computing Systems, p.222, May 19-22, 2003
[12] G. Tsirtsis, G. Giaretta, H. Soliman, and N. Montavont, Traffic selectors for flow bindings (RFC 6088), 2011
[13] G. Tsirtsis, H. Soliman, N. Montavont, Giaretta, G., N. Montavont, and K. Kuladinithi, Flow bindings in mobile IPv6 and NEMO basic support (RFC 6089), 2010
[14] R. Wakikawa, V. Devarapalli, G. Tsirtsis, T. Ernst, and K. Nagami, Multiple care-of addresses registration (RFC 5648), 2009
[15] 802.11 Wireless Networks, The Definitive Guide; Matthew S. Gast, 2nd Edition O'reilly publications
[16] J. Klaue, B. Rathke, and A. Wolisz, EvalVid - A Framework for Video Transmission and Quality Evaluation, In Proc. of the 13th International Conference on Modeling Techniques and Tools for Computer Performance Evaluation, pp. 255-272, Illinois, USA, Sept. 2003
[17] Recommendation ITU-T G.722.2, Wideband coding of speech at around 16 kbit/s using Adaptive Multi-Rate Wideband (AMR-WB), Approved in July 2003
[18] U. Toseef, M. Li, A. Balazs, X. Li, A. Timm-Giel and C. Görg, Investigating the Impacts of IP Transport Impairments on VoIP service in LTE Networks, in 16th VDE/ITG Fachtagung Mobilkommunikation, Osnabrück, Germany, May 18-19, 2011
[19] 3GPP Technical Report TS 23.402, Architecture enhancements for non-3GPP accesses, 3rd Generation Partnership Project, v10.6.0, Dec. 2011
[20] OPNET website, http://www.opnet.com, as accessed in Sept. 2012

 ISBN: 978-1-61208-231-8

Enhanced Positioning Method using WLAN RSSI Measurements considering Dilution of Precision of AP Configuration

Cong Zou, A Sol Kim, Jun Gyu Hwang, Joon Goo Park
Graduate School of Electrical Engineering and Computer Science
Kyungpook National University
Daegu, Republic of Korea
Email: {zoucongmm@naver.com, asoli@hanmail.net, cjstk891015@naver.com, jgpark@ee.knu.ac.kr}

***Abstract*–With the development of mobile internet, requirements of positioning accuracy for the LBS (Location Based Service) are becoming more and more higher. The LBS is based on the position of each mobile device. So, it requires a proper acquisition of accurate user's indoor position. Thus, indoor positioning technology and its accuracy is crucial for various LBS (Location Based Service). In general, RSSI (Received Signal Strength Indicator) measurements are used to obtain the position information of mobile unit under WLAN environment. However, indoor positioning error increases as multiple AP's configurations are becoming more complex. To overcome this problem, an enhanced indoor localization method by AP (Access Point) selection criteria adopting DOP (Dilution of Precision) is proposed. The proposed method can raise the positioning performance according the status of AP distribution.**

Keywords-Indoor positioning; Wireless LAN; RSSI; Dilution of Precision (DOP).

I. INTRODUCTION

Positioning technology is divided into two parts, which are indoor positioning and outdoor positioning respectively. In outdoor positioning, dominant technology is existed such as GPS (Global Positioning System) [1], however, in indoor environments cannot be carried out effectively by it. In recent years, WLAN (Wireless Local Area Network) is widely used to locate in an indoor environment.

Positioning in Wireless Local Area Network (WLAN) based on IEEE802.11 [2] is considered. Generally, received signal strength indication (RSSI) is used in the WLAN Location Based Server (LBS) as the location information provider. However, positioning error usually occurs in indoor environment. Because the access points are set very concentrated and complex in indoor environment. To overcome this problem, in this paper, an enhanced indoor positioning method by access point (AP) configuration selection criteria adopting dilution of precision (DOP) is proposed.

There are a number of existing location systems which utilize a variety of sensing technologies and system architectures. These systems have varying characteristics, such as accuracy, scalability, range, power consumption and cost. Infrared has been popularly used for containment-based location systems [3]. Infrared location system can suffer in strong sunlight an under fluorescent tube lighting as both of these are sources of infrared light. The method that uses RSSI for localization is called fingerprinting. This technique is based on the specific behavior of radio signals in a given environment, including reflections, fading and so on, rather than on the theoretical strength-distance relation. Cricket [4] is an indoor location system developed at MIT and utilizes Radio Frequency (RF) and ultrasound using static transmitters and mobile receives. The Dolphin system [5], developed at the University of Tokyo, utilizes Radio Frequency (RF) and ultrasound to create a peer-to-peer system, providing co-ordinate based positioning. The Dolphin team has created a system which can propagate locations with 10-15cm of accuracy from four stationary reference nodes.

There have been several studies about indoor positioning method adopting dilution of precision (DOP). Ziari et al. [6] present a mathematical approach of a new version of the known GPS dilution of precision and also present a model that allows to estimate the precision based on criteria other than the geometric one only. Lemelson et al. [7] has implemented an algorithm that computes a GPS-like DOP value based on the geometry of access points. In A.G. Dempster [8], positioning using Angle-of-arrival (AOA) and an expression for dilution of dilution of precision (DOP) has been derived for angle-of-arrival positioning systems which allows the quality of an Angle-of-arrival (AOA) position to be determined. Indoor positioning error increases as multiple access point's configurations are becoming more complex. To overcome this problem, in this paper, we propose an indoor positioning method that selects the AP combination adopting DOP due to access point (AP) geometry. That means the selected access point (AP) combination not only has high RSSI but also has good configuration to enhanced positioning precision.

The remaining paper is organized as following. In Section II we discuss general characteristics of DOP and RSSI measurements. Proposed positioning method considering DOP is stated in Section III. In Section IV, the result of experiment is described. Finally, in the Section V, we give conclusion of this paper.

 ISBN: 978-1-61208-231-8

II. CHARACTERISTICS OF DOP AND RSSI MEASUREMENTS

A. Dilution of Precision (DOP)

The effect of satellite geometry is quantified in the measure called Dilution of Precision, or DOP [9]. DOP does not depend on the anything that cannot be predicted in advance. It only depends on the positions of the GPS satellites relative to the GPS location of the receiver. The satellite position is known in advance, and GPS position is also fixed, thus the DOP of GPS system can be calculated even without using the GPS system.

How can we define the DOP is poor or good due to satellite geometry? When satellites are located at wide angles relative to each other, this configuration minimizes the error in position calculations. On the other hand, when satellites are grouped together or located in a line the geometry will be poor. DOP is often divided into several components which are listed below [10]:

VDOP: Vertical DOP
HDOP: Horizontal DOP
PDOP: Positional DOP
TDOP: Time DOP
GDOP: Geometric DOP

These components are used due to the variation of accuracy of the GPS system. The PDOP is most used among other components. The positioning error of PDOP is calculated from the data of GPS receiver multiplied by range error which is given as:

$$\text{Positioning Error} = \text{Range Error} * \text{PDOP} \quad (1)$$

A DOP of 2 means that whatever the range error were, the final positioning error will twice as big. For example, if the user estimated range error (UERE) is 20 meters and the PDOP is 2, the final positioning error will be 40 meters (20 x 2).

B. Computation of DOP

As a first step of computing DOP, consider the unit vectors from the receiver to satellite i [11] :

$$\left(\frac{x_i - x}{R_i}, \frac{y_i - y}{R_i}, \frac{z_i - z}{R_i}\right) \quad (2)$$

where:

$$R_i = \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2}$$

x, y, z : position of the receiver
x_i, y_i, z_i : position of satellite

The formula (2) in matrix form is given by:

$$A = \begin{bmatrix} \frac{x_1 - x}{R_1} & \frac{y_1 - y}{R_1} & \frac{z_1 - z}{R_1} & -1 \\ \frac{x_2 - x}{R_2} & \frac{y_2 - y}{R_2} & \frac{z_2 - z}{R_2} & -1 \\ \frac{x_3 - x}{R_3} & \frac{y_3 - y}{R_3} & \frac{z_3 - z}{R_3} & -1 \\ 1 & 1 & 1 & -1 \end{bmatrix} \quad (3)$$

The first three elements of each row of A are the components of a unit vector form the receiver to the indicated satellite. The elements of the fourth row when consider the fourth satellite. Since the number of AP is three for indoor positioning, thus we assume the fourth AP at the infinite and set every element to 1.

Formulate the matrix, Q, as:

$$Q = (A^T A)^{-1} = \begin{bmatrix} d_x^2 & d_{xy}^2 & d_{xz}^2 & d_{xt}^2 \\ d_{xy}^2 & d_y^2 & d_{yz}^2 & d_{yt}^2 \\ d_{xz}^2 & d_{yz}^2 & d_z^2 & d_{zt}^2 \\ d_{xt}^2 & d_{yt}^2 & d_{zt}^2 & d_t^2 \end{bmatrix} \quad (4)$$

From Q, the DOP can be calculated as:

$$PDOP = \sqrt{d_x^2 + d_y^2 + d_z^2} \quad (5)$$

C. RSSI Measurements

The RSSI (Received Signal Strength Indicator) is defined in IEEE 802.11 standard, which is the ratio of transmitter power and received power present in dBm unit. The RSSI has the characteristic that it can decrease exponentially according to the increase of distance. Because of these characteristics, in this paper we used RSSI attenuation model and is given as [12]:

$$\text{RSSI[dbm]} = -(10n \log_{10} d - A) \quad (6)$$

$$\text{distance[m]} = 10^{\frac{\text{RSSI} - A}{-10n}} \quad (7)$$

In (6) the parameter A is the offset which is the measured RSSI value at 1m point apart from AP. And the parameter n is the attenuation factor. This parameter reflect indoor propagation environment. Because the RSSI is a sensitive parameter, it is can affected by environment significantly. In Figure 1 that shows RSSI attenuation as distance.

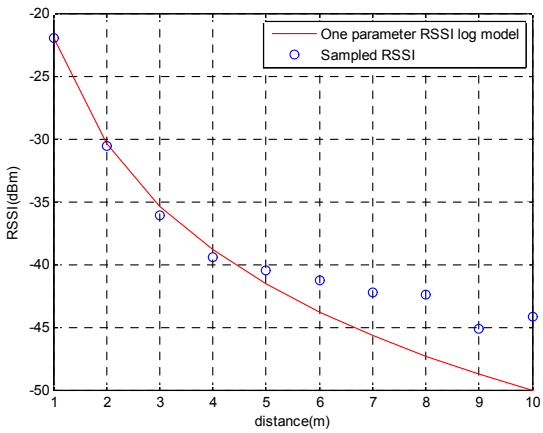


Figure 1. RSSI attenuation according to the elapsed distance.

In practical situations, many factors that can affect RSSI value exist such as furniture, walls and person. These factors can produce signal scattering and multi-path effect. It also can result in positioning error. In order to reduce positioning error, proper parameter determination is necessary.

 ISBN: 978-1-61208-231-8

III. PROPOSED POSITIONING METHOD CONSIDERING DOP

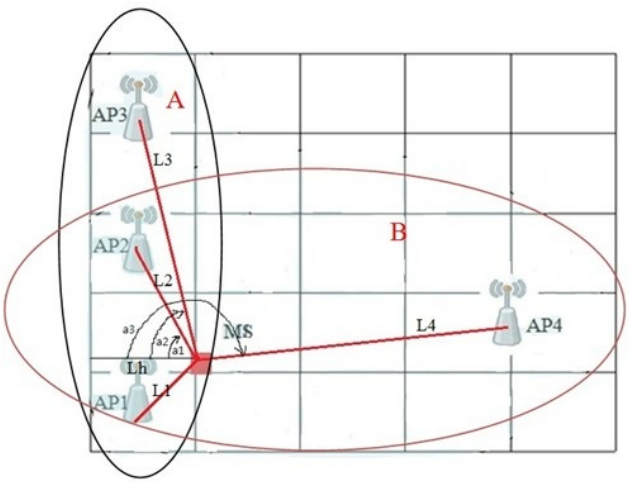
First of all, we should understand the relationship of positioning error between RSSI measurements and DOP, separately. High RSSI value and low DOP can potentially increase the positioning accuracy. Thus, according to above statement, if we can select the AP combination that can produce RSSI value which is high and DOP value is low, then we can get a higher positioning accuracy. However, it is difficult to satisfy all conditions simultaneously. In order to overcome the problem, we consider the appropriate Trade-off between RSSI measurements and DOP. So, we should establish the relationship of positioning error between RSSI and DOP.

In order to get a lower positioning error, we will select the AP whose RSSI value size just be considered in descending order. As shown in Figure 2, we use wireless network card on notebook computer, and inSSIDer software to receive the RSSI from AP1, AP2, AP3, AP4, separately. We use the (5) to calculate the DOP for every AP. The received RSSI values from inSSIDer software are shown in Table 1 as follows:

TABLE 1. Received RSSI value(dBm)

	RSSI value
AP1	-51
AP2	-52
AP3	-70
AP4	-73

When visible access points (APs) are close together or located in a line , the distribution of AP is said to be weak and the DOP value is high, when far apart, the distribution of AP is strong and the DOP is low. As shown as Figure 2, AP1,AP2, and AP3 are located in a line, the DOP value of range A is high, howerver, the DOP of range B is low because the access points (APs) are far from each other.



AP(access point), MS(Mobile Station)
L1: line between AP1 and MS L2: line between AP2 and MS
L3: line between AP3 and MS L4: line between AP4 and MS
Lh: horizon line a1: angle between L2 and Lh
a2: angle between L3 and Lh a3: angle between L4 and Lh

Figure 2. AP selection criteria (1).

However, there are many different configurations of access point (AP) combination, such as combination A of AP1, AP2 and AP3, combination B of AP1, AP2 and AP4 or combination C of AP1, AP3 and AP4 and so on. In general, if don't consider the DOP, the best AP selection is that every access point (AP) has a relative high RSSI value. The Table 1 shows that the RSSI of AP3 is just a little greater than AP4. So, that we should select the combination A to locate can get a higher positioning precision than selecting the combination B. But, according to the description of DOP, we can know that APs are grouped together or located in a line the geometry will be poor and located at wide angles relative to each other, this configuration minimizes the error in position calculations. So if adopting DOP, we should select combination B to locate because the RSSI value of AP4 approximate AP3 and configuration status of AP4 is better than AP3. Why do not select the combination C to locate? In Figure 2, the angle a2 is a little larger than angle a1, so the DOP value of AP3 is a little lower than AP2's, but the Table 1 shows the RSSI value of AP2 is much higher than AP3's. In other words, the difference of DOP between AP2 and AP3 is not high, but the difference of RSSI value between AP2 and AP3 is very high. In this case, it is better that select the AP2 to locate. Finally, we can determine that positioning accuracy B is higher than A. As shown as Figure 3.

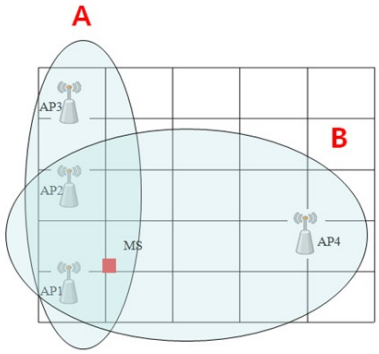


Figure 3. AP selection criteria (2).

Through the analysis of the positioning error, we can find the relationship between RSSI differences and DOP differences. So, we can decide the new AP combination set compared with that of the existing AP set which decided only by RSSI differences.

In Figure 3, because the RSSI value of AP4 approximate AP3, so the RSSI differences between the AP3 and AP4 are not high, and configuration status of AP4 is better than AP3. Namely, the DOP value of AP4 is lower than AP3. Say it again, if we select the AP which is affected by the ratio of RSSI differences and DOP differences, that means the AP has high RSSI and low DOP, then we can get a good positioning result. The relationship between RSSI differences and DOP differences can be given by:

$$\frac{(RSSI3 - RSSI4)}{(DOP3 - DOP4)} > \alpha > 0 \qquad (8)$$

RSSI3, RSSI4: The RSSI of 3rd and 4th AP

 ISBN: 978-1-61208-231-8

DOP3, DOP4: the DOP of 3rd and 4th AP

α : Threshold value which is determined by environments

According to (8), if the ratio of RSSI differences and DOP differences is greater than the threshold value which is determined by environments, we will select the new AP to compare, otherwise, using the existing AP to locate.

The algorithm is shown as follows:

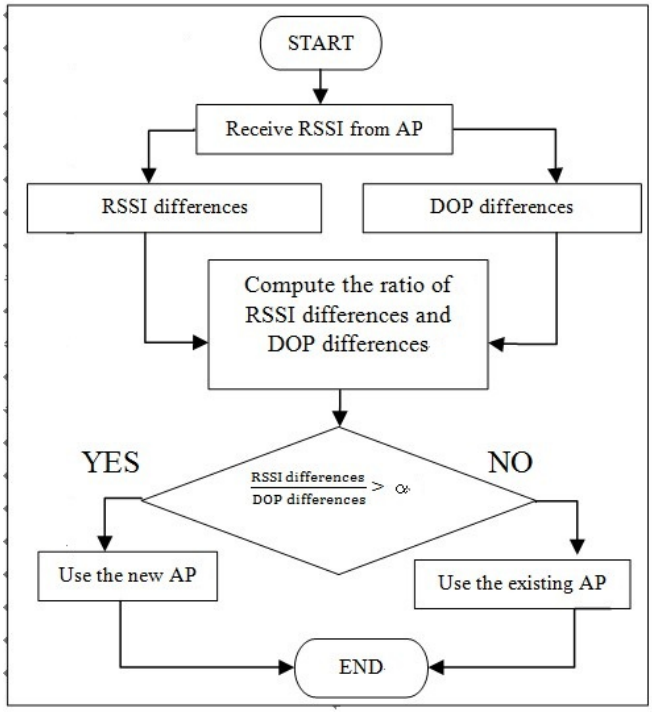


Figure 4. The proposed positioning algorithm.

IV. EXPERIMENTAL RESULT

We verify the result by experiment in indoor half-open environment. In this experiment, the threshold value α is 1.8.

In Figure 5. (a), it shows the distribution of access points (APs) which are set arbitrarily and the path of mobile station (MS). In Figure 5. (b), it can easy find that the positioning error of MS1 adopting DOP is better than the positioning error without adopting DOP. The same situation occurs in MS2 and MS3. But in the adopting DOP and without adopting DOP case, the result is almost the same.

In Figure. 5 (a), we can find that the access points (APs) around the MS1, MS2, MS3 are very concentrated. If we do not adopt DOP to calculate the position of MS1, MS2 and MS3, we certainly select the combination of AP1, AP2 and AP3, because the RSSI value of AP1, AP2 and AP3 are better than others. If we adopt DOP to calculate the position of MS1, MS2 and MS3, we will select the combination of AP1, AP2 and AP5 to calculate the position of MS1, and that calculate the position of MS2 will select the combination of AP2, AP3 and AP4. According to the result, if the access points are set very concentrated and complex in indoor environment, the positioning error of adopting DOP is lower than without adopting DOP.

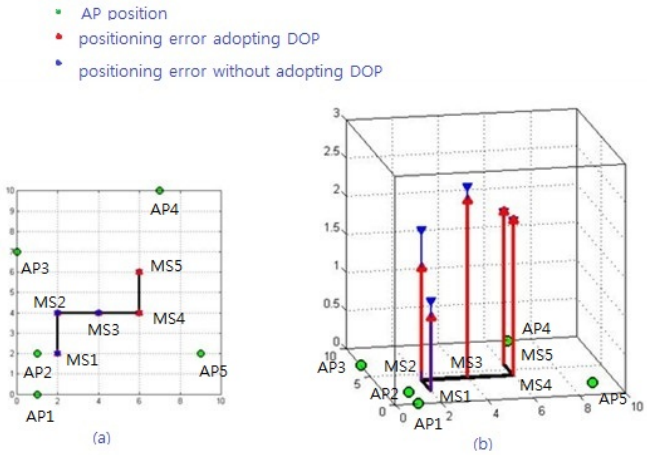


Figure 5. Experiment result comparison: (a) MS path and AP position distribution. (b) Comparison of positioning error adopting DOP and positioning error without adopting DOP.

As shown as Table 2, the positioning error of proposed method is less than that of existing method by 9.3%. The existing method using RSSI attenuation model in WLAN environment.

TABLE 2. position error experiment result (m)

	Existing Method	Proposed Method
Average error	1.93	1.75
Minimum error	1.18	0.96
Maximum error	2.50	2.32

V. CONCLUSION

This paper described a method for indoor positioning use the RSSI attenuation model in WLAN environment. In order to enhanced indoor positioning accuracy, we adopt DOP (Dilution of Precision). That we can analyze the ratio relationship between RSSI differences and DOP differences of each AP to select the AP combination with high RSSI and low DOP. That is, it can raise the positioning performance according the status of AP distribution. Positioning error usually occurs in indoor environment. Because the access points are set very concentrated and complex in indoor environment. In this paper, proposed method can raise accuracy in access point distribution concentrated and complex indoor environment. The experimental result shows that the positioning error of proposed method adopting DOP is less than that of existing method only use RSSI attenuation model by 9.3%.

ACKNOWLEDGMENT

This work has been supported by National GNSS Research Center program of Defense Acquisition Program Administration and Agency for Defense Development.

 ISBN: 978-1-61208-231-8

REFERENCES

[1] M. Wright, D. Stallings, and D. Dunn, "The effectiveness of global positioning system electronic navigation," SoutheastCon, 2003. Proceedings. IEEE, pp. 62-67, 4-6 April 2003.

[2] IEEE Standard for Information Technology, Telecommunications and Information Exchange Between Systems, Local and Metropolitan Area Network. Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Standard 802.11, 1999.

[3] http://www.ubisense.net, October 2012.

[4] N.B. Priyantha, A. Chakraborty, and H. Balakrishnan, "The cricket location-support system," In Proceedings of the 6th annual international conference on Mobile computing and networking, pp. 32-43, ACM Press, 2000.

[5] Y. Fukuju, M. Minami, H. Morikawa, and T. Aoyama. "Dolphin: An autonomous indoor positioning system in ubiquitous computing environment," In IEEE Workshop on Software Technologies for Future Embedded System (WSTFES2003), pp. 53-56, Hakodate, Japan, May 2003.

[6] S. Zirari, P. Canalda, and F. Spies, "Geometric and Singal Strength Dilution of Precision (DOP) Wi-Fi," IJCSI International Journal of Coputer Science Issues, Vol. 3, pp. 35-44, 2009.

[7] H. Lemelson, M. B. Kjargaard, R Hansen, and T. King, "Error Estimation for Indoor 802.11 Location Fingerprinting," LoCA '09 Proceedings of the 4th International Symposium on Location and Context Awareness, pp. 138-155, 7-8 May 2009.

[8] A.G. Dempster, "Dilution of precision in angle-of-arrival positioning systems"Electronics Letters 2nd March 2006 Vol. 42 No. 5, Electronic Letters online no.: 20064410, pp. 291-292.

[9] Frederic G. Snider, R.P.G, "GPS: Theroy, Practice and Applications," http://www.pdhcenter.com, PDH Course L116, October, 2012.

[10] http://gpsinformation.net/main/dopnontech.htm, October 2012.

[11] http://en.wikipedia.org/wiki/Dilution_of_precision_(GPS), October 2012.

[12] S. Park, D. Park, A. S. Kim, J. Park, S. Kim, C. Lim, and J. G. Park, "A Study on enhanced indoor localization method through IEEE 802.11 signal strength measurement" KSII The second International Conference on Internet (ICONI) 2010, pp. 761- 765, December 2010.

 ISBN: 978-1-61208-231-8

TCP, UDP and FTP Performance Measurements of IEEE 802.11 a, g Laboratory WEP and WPA Point-to-Point Links

José A. R. Pacheco de Carvalho[1,2], Cláudia F. F. Ribeiro Pacheco[1], Hugo Veiga[1,3]
[1]Unidade de Detecção Remota, [2]Dep. de Física,
[3]Centro de Informática
Universidade da Beira Interior
6201-001 Covilhã, Portugal
pacheco@ubi.pt, a17597@ubi.pt, hveiga@ubi.pt

António D. Reis[1,2,4]
[4]Dep. Electrónica e Telecom. / Instituto Telecom.
Universidade de Aveiro
3810 Aveiro, Portugal
adreis@ubi.pt

***Abstract*—The importance of wireless communications, involving electronic devices, has been growing. Performance is a crucial issue, leading to more reliable and efficient communications. Security is equally important. Laboratory measurements were performed on several performance aspects of Wi-Fi (IEEE 802.11 a, g) WEP and WPA point-to-point links. Our study contributes to the performance evaluation of this technology, using available equipments (DAP-1522 access points from D-Link and WPC600N adapters from Linksys). New detailed results are presented and discussed, namely at OSI levels 4 and 7, from TCP, UDP and FTP experiments: TCP throughput, jitter, percentage datagram loss and FTP transfer rate. Comparisons are made to corresponding results obtained for, mainly, open links. Conclusions are drawn about the comparative performance of the links.**

Keywords-IEEE 802.11a, g Point-to-Point Links; WEP; WPA; Wireless Network Laboratory Performance.

I. INTRODUCTION

Contactless communication techniques have been developed using mainly electromagnetic waves in several frequency ranges, propagating in the air. Wireless fidelity (Wi-Fi) and free space optics (FSO), whose importance and utilization have been recognized and growing, are representative examples of wireless communications technologies. Wi-Fi is a microwave based technology providing for versatility, mobility and favourable prices. Wi-Fi has been considerably expanding to complement the traditional wired networks. It has been used both in ad hoc mode and in infrastructure mode. In this case, a wireless local area network (WLAN), based on an access point (AP), permits Wi-Fi electronic devices to communicate with a wired based local area network (LAN) through a switch/router. At the personal home level, a wireless personal area network (WPAN) permits personal devices to communicate. Point-to-point and point-to-multipoint 2.4 and 5 GHz microwave links are used, with IEEE 802.11a, 802.11b, 802.11g and 802.11n standards [1]. Nominal transfer rates up to 11 (802.11b), 54 Mbps (802.11 a, g) and 600 Mbps (802.11n) are specified. Carrier sense multiple access with collision avoidance (CSMA/CA) is the medium access control. There are studies on wireless communications, wave propagation [2,3], practical implementations of WLANs [4], performance analysis of the effective transfer rate for 802.11b point-to-point links [5], 802.11b performance in crowded indoor environments [6].

Performance has been a very important issue, resulting in more reliable and efficient communications. In comparison to traditional applications, new telematic applications are especially sensitive to performances. Requirements have been pointed out [7].

Wi-Fi security is very important. Microwave radio signals can be very easily captured as they travel through the air. Therefore, several security methods have been developed to provide authentication such as, by increasing order of security, wired equivalent privacy (WEP), Wi-Fi protected access (WPA) and Wi-Fi protected access II (WPA2). WEP was initially intended to provide confidentiality comparable to that of a traditional wired network. A shared key for data encryption is involved. The communicating devices use the same key to encrypt and decrypt radio signals. The cyclic redundancy check 32 (CRC32) checksum used in WEP does not provide a great protection. However, in spite of its weaknesses, WEP is still widely used in Wi-Fi communications for security reasons, mainly in point-to-point links. WPA implements the majority of the IEEE 802.11i standard [1]. It includes a message integrity code (MIC), replacing the CRC used in WEP. Either personal or enterprise modes can be used. In this latter case an 802.1x server is required. Both temporal key integrity protocol (TKIP) and advanced encryption standard (AES) cipher types are usable and a group key update time interval is specified.

Several performance measurements have been made for 2.4 and 5 GHz Wi-Fi open [8-9], WEP [10], WPA links [11], as well as very high speed FSO [12]. It is important to investigate the effects of increasing levels of security encryption on link performance. Therefore, in the present work new Wi-Fi (IEEE 802.11 a, g) results arise, using personal mode WPA, through OSI levels 4 and 7. Performance is evaluated in laboratory measurements of WPA point-to-point links using new available equipments. Comparisons are made to corresponding results obtained for WEP and open links.

The rest of the paper is structured as follows: Section II describes the state of the art, the problem and the solution.

 ISBN: 978-1-61208-231-8

Section III presents the experimental details i.e. the measurement setup and the procedure. The results and discussion are presented in Section IV. Conclusions are drawn in Section V.

II. State of the Art, Problem and Solution

In prior and actual state of the art, several Wi-Fi connections have been studied and implemented. Performance evaluation has been considered as a fundamentally important criterion to assess communications quality. The motivation of this work is to evaluate performance in laboratory measurements of WPA point-to-point links using new available equipments. Comparisons are made to corresponding results obtained for WEP and open links. This contribution permits to increase the knowledge about performance of Wi-Fi (IEEE 802.11 a,g) point-to-point links [4-6]. The problem statement is that performance needs to be evaluated under security encryption. The solution proposed uses an experimental setup and method, permitting to monitor signal to noise ratios (SNR) and noise levels (N) and measure TCP throughput (from TCP connections) and UDP jitter and percentage datagram loss (from UDP communications).

III. Experimental Details

The measurements used a D-Link DAP-1522 bridge/access point [13], with internal PIFA *2 antenna, IEEE 802.11 a/b/g/n, firmware version 1.31 and a 100-Base-TX/10-Base-T Allied Telesis AT-8000S/16 level 2 switch [14]. The wireless mode was set to access point mode. The firmware from the manufacturer did not make possible a point-to-point link with a similar equipment. Therefore, a personal computer (PC) was used having a PCMCIA IEEE.802.11 a/b/g/n Linksys WPC600N wireless adapter with three internal antennas [15], to enable a PTP link to the access point. In every type of experiment, interference free communication channels were used (ch 36 for 802.11a; ch 8 for 802.11g). This was checked through a portable computer, equipped with a Wi-Fi 802.11 a/b/g/n adapter, running NetStumbler software [16]. WPA personal encryption was activated in the AP and the PC wireless adapter using AES and a shared key with 26 ASCII characters. WEP encryption was activated in both equipments, using 128 bit encryption and a key composed of 26 ASCII characters. The experiments were made under far-field conditions. No power levels above 30 mW (15 dBm) were required, as the access points were close.

A laboratory setup has been planned and implemented for the measurements, as shown in Fig. 1. At OSI level 4, measurements were made for TCP connections and UDP communications using Iperf software [17]. For a TCP connection, TCP throughput was obtained. For a UDP communication with a given bandwidth parameter, UDP throughput, jitter and percentage loss of datagrams were determined. Parameterizations of TCP packets, UDP datagrams and window size were as in [10]. One PC, with IP 192.168.0.2 was the Iperf server and the other, with IP 192.168.0.6, was the Iperf client. Jitter, representing the smooth mean of differences between consecutive transit times, was continuously computed by the server, as specified by the real time protocol (RTP), in RFC 1889 [18]. The scheme of Fig. 1 was also used for FTP measurements, where the FTP server and the client applications were installed in the PCs with IPs 192.168.0.2 and 192.168.0.6, respectively. The server PC also permitted manual control of the settings in the access point.

The server and client PCs were HP nx9030 and nx9010 portable computers, respectively, running Windows XP. They were configured to optimize the resources allocated to the present work. Batch command files have been written to enable the TCP, UDP and FTP tests. The results were obtained in batch mode and written as data files to the client PC disk. Each PC had a second network adapter, to permit remote control from the official IP University network, via switch.

IV. Results and Discussion

The access point and the PC wireless network adapter were manually configured, for both standards IEEE 802.11 a, g, with typical fixed transfer rates (6, 9, 12, 18, 24, 36, 48, 54 Mbps). For every fixed transfer rate, data were obtained for comparison of the laboratory performance of the links at OSI layers 1 (physical layer), 4 (transport layer) and 7 (application layer) using the setup of Fig. 1. For each standard and every nominal fixed transfer rate, an average TCP throughput was determined from several experiments. This value was used as the bandwidth parameter for every corresponding UDP test, giving average jitter and average percentage datagram loss.

At OSI level 1, noise levels (N, in dBm) and signal to noise ratios (SNR, in dB) were monitored and typical values are shown in Fig. 2 and Fig. 3 for WPA and WEP links, respectively. They are similar to those obtained for open links.

The main average TCP and UDP results are summarized in Table I, both for WPA and open links. The statistical analysis, including calculations of confidence intervals, was carried out as in [19]. In Figs. 4-5, polynomial fits were made (shown as y versus x), using the Excel worksheet, to the 802.11 a, g TCP throughput data for WPA and open links, respectively, where R^2 is the coefficient of determination. It provides information about the goodness of fit. If it is 1.0, it indicates a perfect fit to data. It was found that the best TCP throughputs are for 802.11 a, for every link type, where the best SNR values were measured. The 802.11 a, g average data are reasonably close for all link types. The best average 802.11g TCP throughput is for open links. In Figs. 6-10, the data points representing jitter and percentage datagram loss were joined by smoothed lines. The jitter data show some fluctuations in some cases, mainly for 802.11a, as seen in Figs. 6 and 8. It was found that, on average, the best jitter performances are for 802.11 g for all link types. On average, for both 802.11 a and 802.11 g, the jitter performances were not found significantly sensitive, within the experimental errors, to link type. In Figs. 9-10, where percentage datagram loss data are shown, the error bars are well visible.

 ISBN: 978-1-61208-231-8

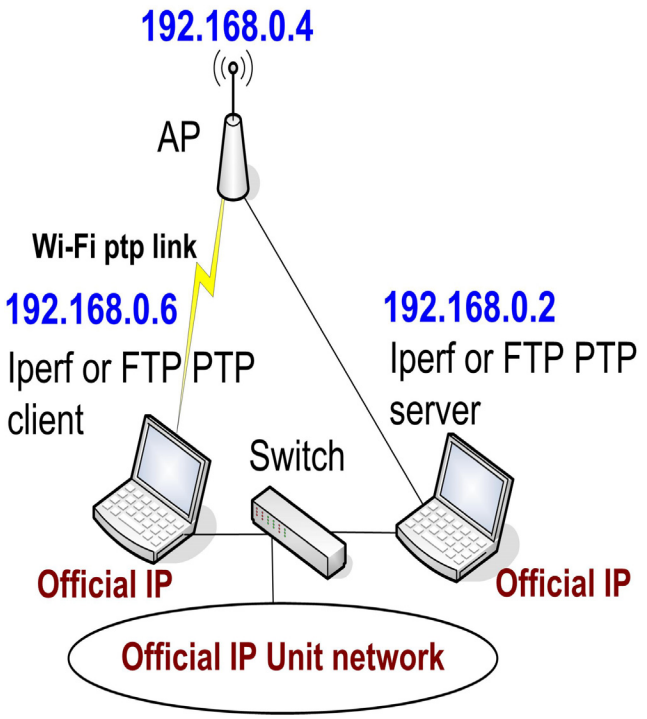


Figure 1. Laboratory setup scheme.

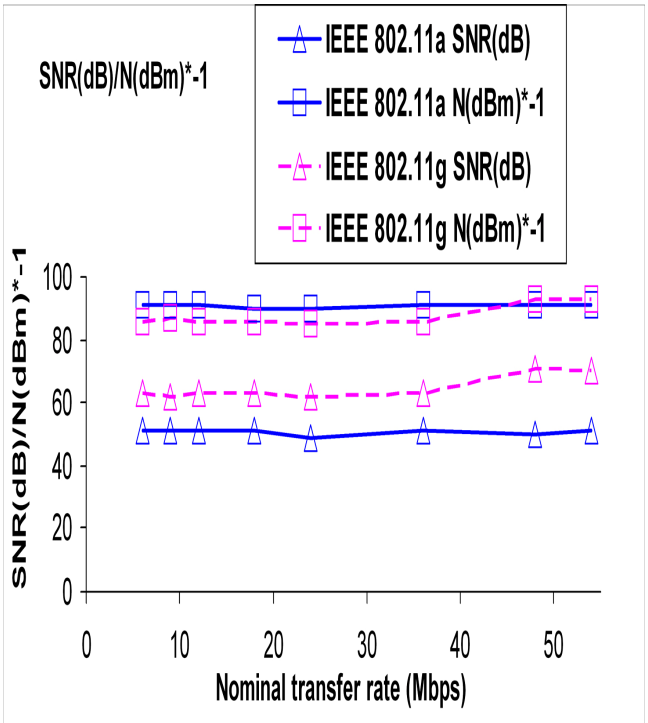


Figure 2. Typical SNR (dB) and N (dBm). WPA links.

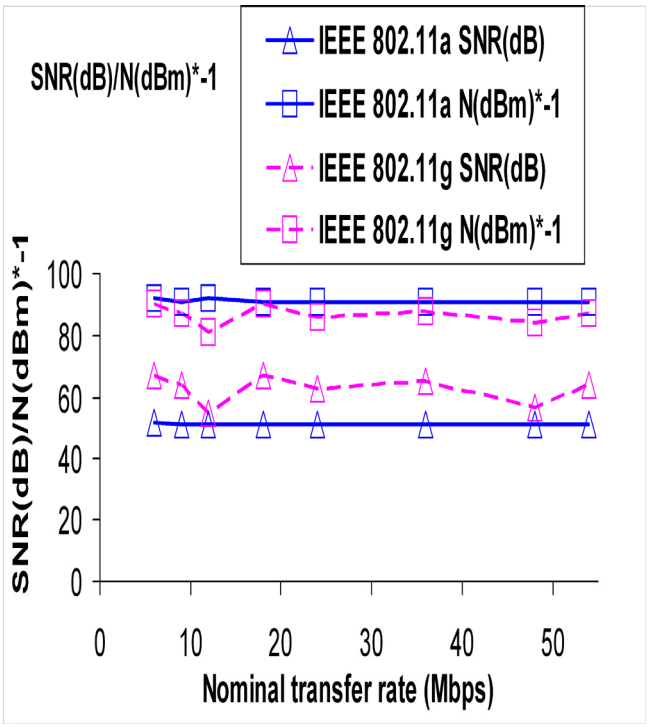


Figure 3. Typical SNR (dB) and N (dBm). WEP links.

TABLE I. AVERAGE WI-FI (IEEE 802.11 A, G) RESULTS; WPA AND OPEN LINKS

Link type	**WPA**		**Open**	
Parameter/ IEEE standard	***802.11a***	***802.11g***	***802.11a***	***802.11g***
TCP throughput (Mbps)	15.9 +-0.5	13.4 +-0.4	15.7 +-0.5	14.5 +-0.4
UDP-jitter (ms)	2.5 +-0.5	2.3 +-0.1	2.8 +-0.2	2.3 +-0.1
UDP-% datagram loss	1.2 +-0.2	1.8 +-0.2	0.7 +-0.1	1.2 +-0.1
FTP transfer rate (kbyte/s)	1765.4 +-70.7	1450.6 +-58.0	1745,2 +-69.8	1526.9 +-61.1

 ISBN: 978-1-61208-231-8

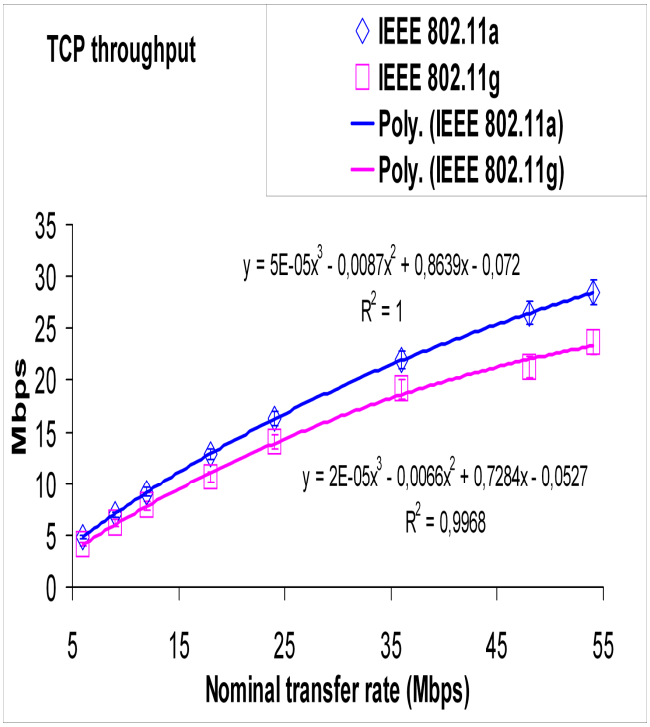


Figure 4. TCP throughput (y) versus technology and nominal transfer rate (x). WPA links.

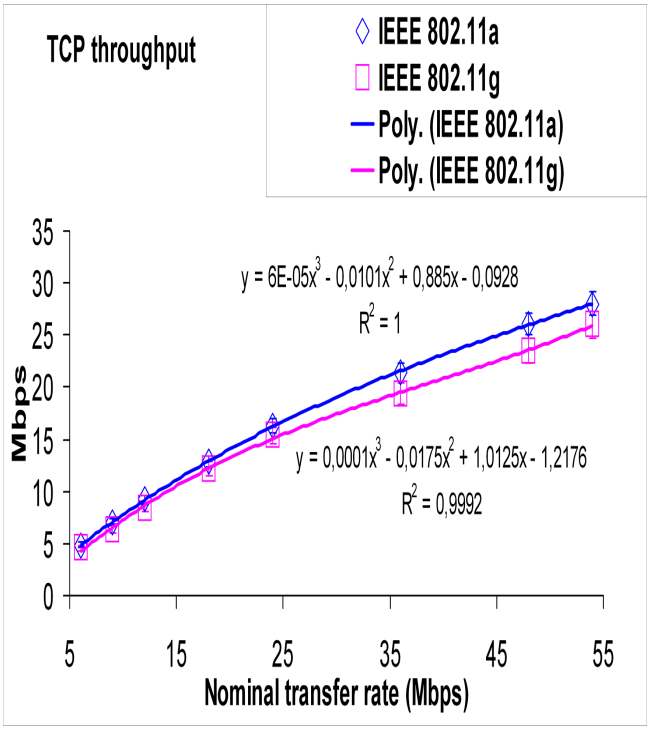


Figure 5. TCP throughput (y) versus technology and nominal transfer rate (x). Open links.

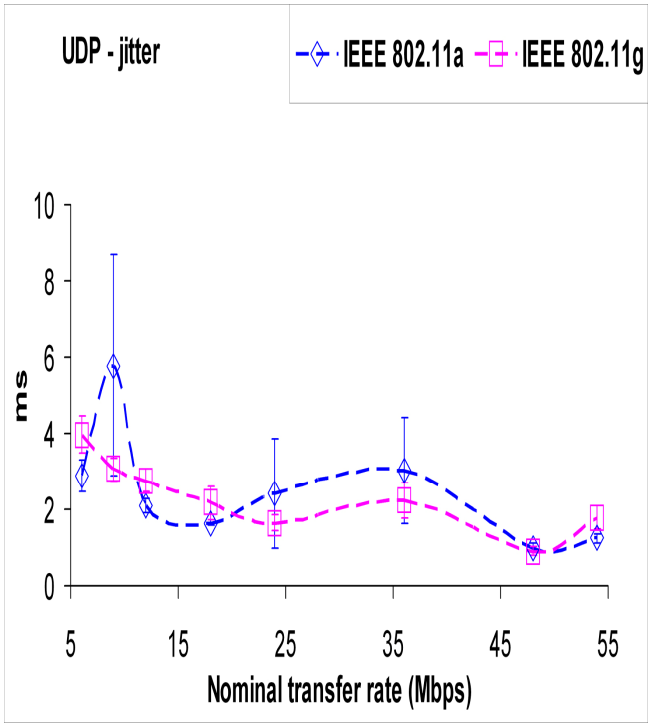


Figure 6. UDP – jitter results versus technology and nominal transfer rate. WPA links.

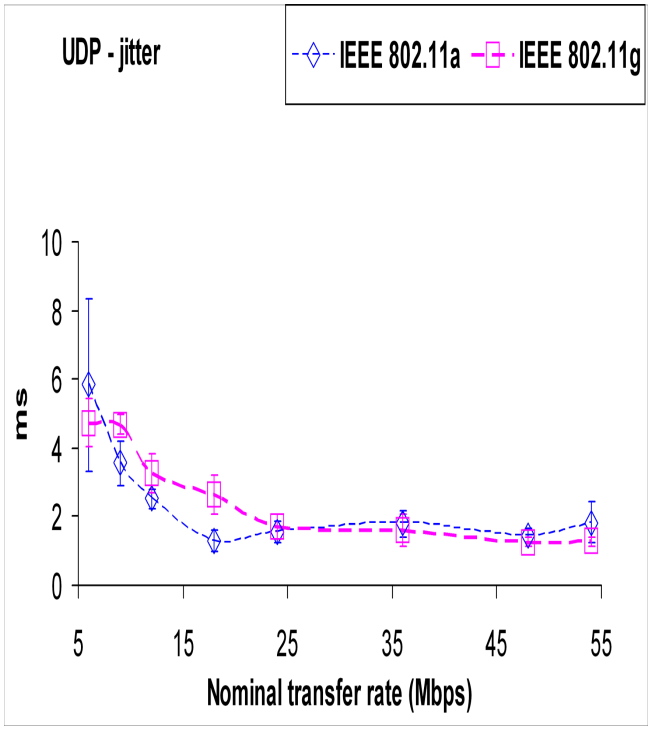


Figure 7. UDP – jitter results versus technology and nominal transfer rate. WEP links.

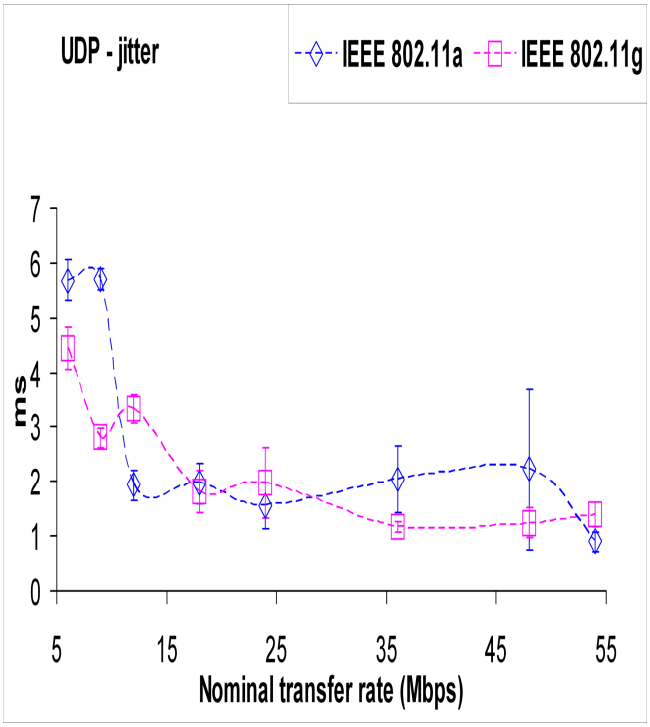


Figure 8. UDP – jitter results versus technology and nominal transfer rate. Open links.

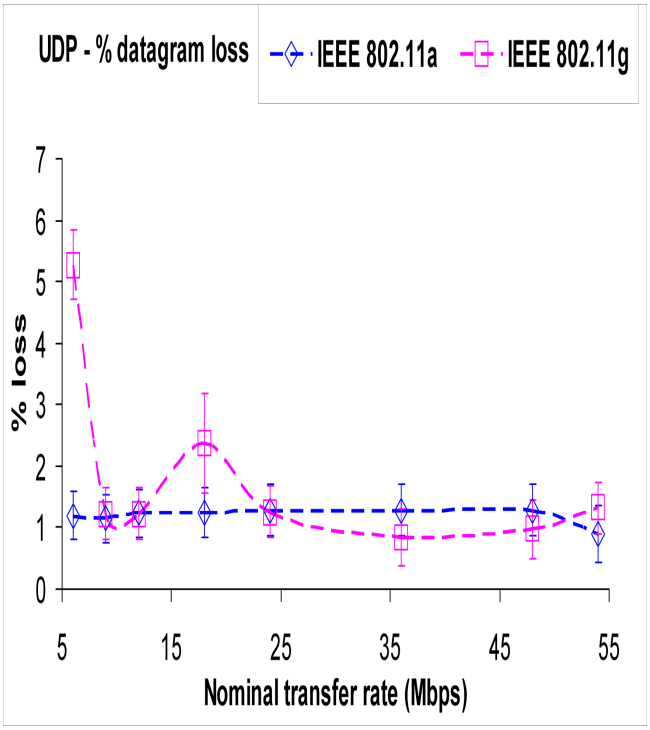


Figure 9. UDP – percentage datagram loss results versus technology and nominal transfer rate. WPA links.

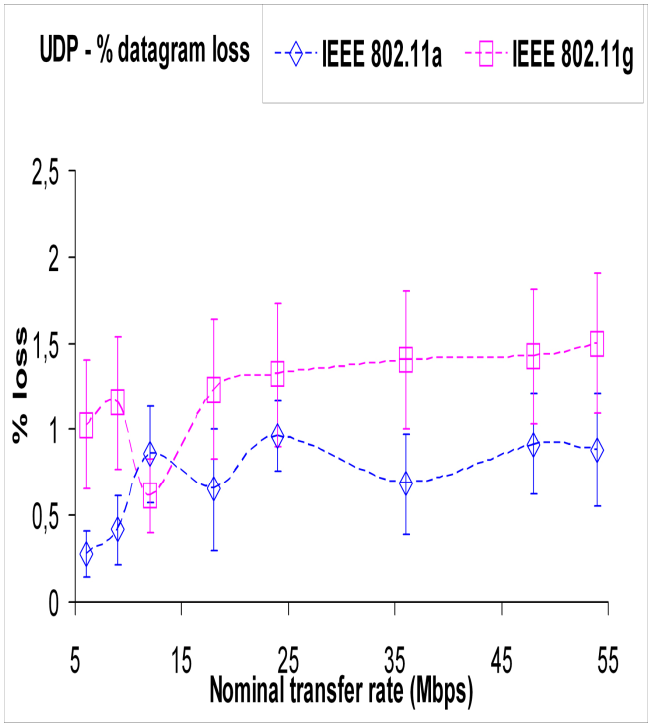


Figure 10. UDP – percentage datagram loss results versus technology and nominal transfer rate. Open links.

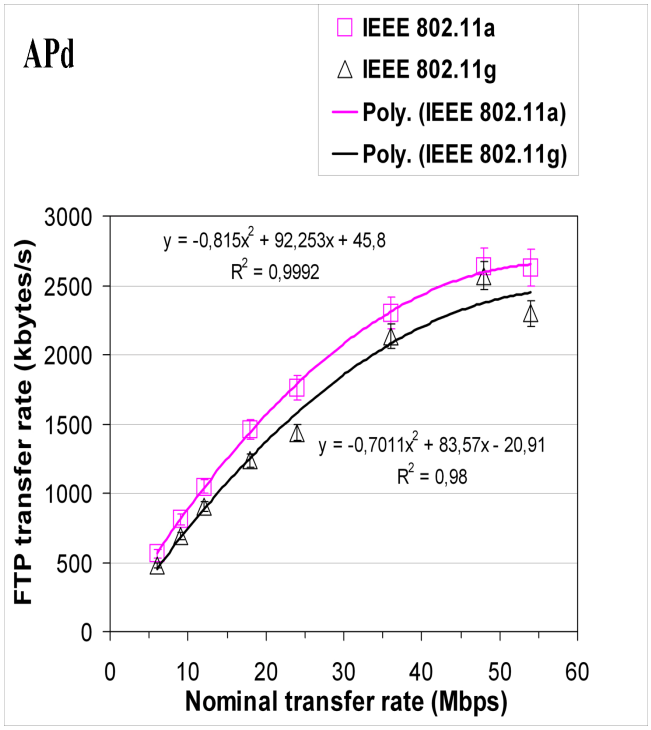


Figure 11. FTP transfer rate (y) versus technology and nominal transfer rate (x). WEP links.

The best performances were for 802.11 a for both link types. Increasing security encryption was found to degrade performance for both standards 802.11 a,g. This is expected due to increased data length.

At OSI level 7, we measured the FTP transfer rates versus nominal transfer rates configured in the access points for IEEE 802.11 a, g as in [11]. The average results thus obtained are summarized in Table I, both for WPA and open links. In Fig. 11 polynomial fits are shown to 802.11 a, g data for WEP links. The results show the same trends found for TCP throughput.

Generally, except for 802.11g TCP throughput and 802.11 a,g percentage datagram loss, where increasing security encryption was found to degrade performances, the results measured for WPA links were found to agree, within the experimental errors, with corresponding data obtained for all link types.

V. CONCLUSION AND FUTURE WORK

A new laboratory setup arrangement has been planned and implemented, that permitted systematic performance measurements of new available wireless equipments (DAP-1522 access points from D-Link and WPC600N adapters from Linksys) for Wi-Fi (IEEE 802.11 b,g) in WPA point-to-point links.

Through OSI layer 4, TCP throughput, jitter and percentage datagram loss were measured and compared for WPA, WEP and open links. It was found that the best TCP throughputs were found for 802.11a, for every link type. Generally, except for 802.11g TCP throughput and 802.11 a,g percentage datagram loss, where increasing security encryption was found to degrade performances, the results measured for WPA links were found to agree, within the experimental errors, with corresponding data obtained for all link types. Jitter performances were not found significantly sensitive, within the experimental errors, to link type.

At OSI layer 7, FTP performance results have shown the same trends found for TCP throughput.

Future performance studies are planned using several equipments, security settings and experimental conditions, not only in laboratory but also in outdoor environments involving, mainly, medium range links.

ACKNOWLEDGMENT

Supports from University of Beira Interior and FCT (Fundação para a Ciência e a Tecnologia)/PEst-OE/FIS/UI0524/2011 (Projecto Estratégico-UI524-2011-2012) are acknowledged.

REFERENCES

[1] Web site http://standards.ieee.org; IEEE 802.11a, 802.11b, 802.11g, 802.11n, 802.11i standards; [retrieved: January, 2012].

[2] J. W. Mark and W. Zhuang, Wireless Communications and Networking, Prentice-Hall, Inc., Upper Saddle River, NJ, 2003.

[3] T. S. Rappaport, Wireless Communications Principles and Practice, 2nd ed., Prentice-Hall, Inc., Upper Saddle River, NJ, 2002.

[4] W. R. Bruce III and R. Gilster, Wireless LANs End to End, Hungry Minds, Inc., NY, 2002.

[5] M. Schwartz, Mobile Wireless Communications, Cambridge University Press, 2005.

[6] N. Sarkar, and K. Sowerby, "High Performance Measurements in the Crowded Office Environment: a Case Study", In Proc. ICCT'06-International Conference on Communication Technology, pp. 1-4, Guilin, China, 27-30 November 2006.

[7] E. Monteiro and F. Boavida, Engineering of Informatics Networks, 4th ed., FCA-Editor of Informatics Ld., Lisbon, 2002.

[8] J. A. R. Pacheco de Carvalho, P. A. J. Gomes, H. Veiga, and A. D. Reis, "Development of a University Networking Project", in Encyclopedia of Networked and Virtual Organizations, Goran D. Putnik, Maria Manuela Cunha, Eds. Hershey, PA (Pennsylvania): IGI Global, pp. 409-422, 2008.

[9] J. A. R. Pacheco de Carvalho, H. Veiga, P. A. J. Gomes, C. F. Ribeiro Pacheco, N. Marques, and A. D. Reis, "Wi-Fi Point-to-Point Links- Performance Aspects of IEEE 802.11 a,b,g Laboratory Links", in Electronic Engineering and Computing Technology, Series: Lecture Notes in Electrical Engineering, Sio-Iong Ao, Len Gelman, Eds. Netherlands: Springer, 2010, Vol. 60, pp. 507-514.

[10] J. A. R. Pacheco de Carvalho, H. Veiga, N. Marques, C. F. Ribeiro Pacheco, and A. D. Reis, Wi-Fi WEP Point-to-Point Links- Performance Studies of IEEE 802.11 a,b,g Laboratory Links, in Electronic Engineering and Computing Technology, Series: Lecture Notes in Electrical Engineering, Sio-Iong Ao, Len Gelman, Eds. Netherlands: Springer, 2011, Vol. 90, pp. 105-114.

[11] J. A. R. Pacheco de Carvalho, H. Veiga, N. Marques, C. F. F. Ribeiro Pacheco, and A. D. Reis, "Performance Measurements of IEEE 802.11 b, g Laboratory WEP and WPA Point-to-Point Links using TCP, UDP and FTP", Proc. Applied Electronics 2011 - 16th International Conference, pp. 293-298, University of West Bohemia, Pilsen, Czech Republic, 7-8 September 2011.

[12] J. A. R. Pacheco de Carvalho, N. Marques, H. Veiga, C. F. F. Ribeiro Pacheco, and A. D. Reis, "Performance Measurements of a 1550 nm Gbps FSO Link at Covilhã City, Portugal", Proc. Applied Electronics 2010 - 15th International Conference, pp. 235-239, Pilsen, Czech Republic, 8-9 September 2010.

[13] Web site http://www.dlink.com; DAP-1522 wireless bridge/access point technical manual; [retrieved: January, 2012].

[14] Web site http://www.alliedtelesis.com; AT-8000S/16 level 2 switch technical data; [retrieved: February, 2012].

[15] Web site http://www.linksys.com; WPC600N notebook adapter user guide; [retrieved: November, 2011].

[16] Web site http://www.netstumbler.com; NetStumbler software; [retrieved: March, 2012].

[17] Web site http://dast.nlanr.net; Iperf software; [retrieved: February, 2007].

[18] Network Working Group. "RFC 1889-RTP: A Transport Protocol for Real Time Applications", http://www.rfc-archive.org; [retrieved: March, 2012].

[19] P. R. Bevington, Data Reduction and Error Analysis for the Physical Sciences, Mc Graw-Hill Book Company, 1969

 ISBN: 978-1-61208-231-8

Real Time FPGA based Testbed for OFDM Development with ML synchronization

Tiago Pereira, Manuel Violas, Atílio Gameiro, Carlos Ribeiro, and João Lourenço
DETI, Instituto de Telecomunicações, University of Aveiro
Aveiro, Portugal
e-mails: targp@av.it.pt, manuelv@ua.pt, amg@ua.pt, cribeiro@av.it.pt, and jlourenco@av.it.pt

Abstract – **In this paper, we present a real-time testbed Orthogonal Frequency Division Multiplexing (OFDM) signaling scheme. The testbed is implemented in a Field-Programmable Gate Array (FPGA) through Xilinx System Generator for DSP and includes all the blocks needed for the transmission path of OFDM. Time-domain synchronization is achieved through a joint maximum likelihood (ML) symbol-time and carrier frequency offset (CFO) estimator through the redundant information contained in the cyclic prefix (CP). Results show that a rough implementation of the signal path can be implemented by using only Xilinx System Generator for DSP. This work presents a valid FPGA implementation of an OFDM receiver synchronization algorithm using a high-level design tool.**

Keywords – OFDM; FPGA; Software Defined Radio (SDR); physical layer; time-domain synchronization.

I. INTRODUCTION

Although multicarrier techniques can be traced back to 1966 [1], the first commercial application of OFDM occurred only in 1995 with the Digital Audio Broadcasting (DAB) standard [2]. OFDM is a multicarrier bandwidth efficiency scheme for digital communications where the main difference to conventional frequency division multiplexing (FDM) is that in the frequency domain the OFDM subcarriers overlap, providing spectrum efficiency. Given that OFDM implementations are carried out in the digital domain, there are a number of platforms able to implement an OFDM system suitable for software defined radio (SDR) development. SDR has been emerging within the wireless industry and can be applied to several applications. It is defined as a radio communication system where some physical (PHY) layer components that are typically implemented in analog hardware (filters, mixers, etc.) are implemented in software instead, thus allowing the user to operate the radio in different environments providing flexibility due to its reconfigurability.

The system presented was built using a high-level design tool built into Matlab's Simulink, Xilinx System Generator for DSP, providing the user with high-level abstractions of the system that can be automatically compiled into an FPGA [10].

Work presented here is divided as follows: Section II presents the literature review, the receiver critical parts and the paper's aim; Section III presents a brief description of the transceiver architecture and the received signal's ambiguities; Section IV is divided in three parts and presents the algorithm implemented for time-domain estimation and compensation; Section V presents the testbed used and how simulations were performed and Section VI explains the simulation results. Conclusions are provided in Section VII.

II. RELATED WORK

Several testbeds for OFDM systems based on SDR have been reported on literature. For example, [3] presents an OFDM modulator/demodulator with two synchronization options and two error-controlling techniques. The work in [4] uses GNU radio to transfer OFDM signals with QPSK and BPSK modulation to analyze the packet-received ratio for Quality of Service purposes. Other broadly adopted research platform is WARP [5]. The work in [6] uses this testbed to present an OFDM-based cooperative system using Alamouti's block code to study its capability versus a 2 x 1 multiple input single output system. FPGA implementations of standards 802.11a and 802.16-2004' modulators using Xilinx System Generator for DSP for high level design can be found in [7][8].

Two critical parts of the receiver are the synchronization and channel estimation subsystems. The synchronization should estimate the frame arrival time and a frequency offset between the local oscillators and RF carriers. Compensation can then be applied to the incoming signal. Unlike IEEE 802.11a/g and 802.16 (WiMax), among others, this system does not use a training sequence to achieve time-domain synchronization.

The aim of this paper is to present the implementation of an FPGA-based OFDM receiver with a ML time-domain synchronization algorithm using Xilinx System Generator for DSP.

III. THE ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING TRANSCEIVER

Figure 1 depicts the transceiver architecture of the system discussed in this paper. On the transmitter, data is generated randomly by making an inverse fast Fourier transform (IFFT) of quadrature amplitude modulated (QAM) symbol sets with 1024 subcarriers. The CP is added after the IFFT and the symbols are turned into frames. An up-conversion of 4 is performed on the interpolation block by a set of two interpolation filters: a square-root-raised-cosine and a halfband. The mixer block performs frequency translation to an intermediate frequency (IF) and is achieved by mixing the frame with a direct digital synthesizer (DDS). On the receiver side another DDS translates the IF back to baseband on the mixer block. Down-conversion and matched filtering is performed by a similar set of filters as the ones used on the

 ISBN: 978-1-61208-231-8

transmitter by the decimator block. Once the estimations for the offsets are performed, the data forwarding control (DFC) and CFO correction blocks perform the compensations. A fast Fourier Transform (FFT) retrieves the data. Several parameters along the system are reconfigurable at user's need. Such parameters include number of symbols per frame, CP length, carrier frequency (limited by the system's frequency), modulation (QPSK, 16-QAM, 64-QAM, etc.) and the system's main clock frequency.

Preventing intersymbol interference (ISI) and preserving subcarrier orthogonality is achieved by adding a preamble of L samples to each symbol that contains the information of the last N samples of each OFDM symbol. Such symbol structure (N+L samples) maintains subcarrier orthogonality, in spite of the loss in transmission power and throughput.

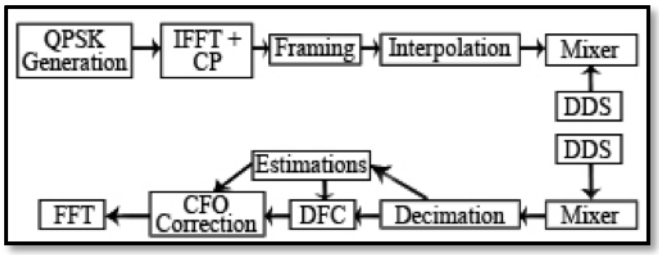


Figure 1. Baseband and IF transceiver arquitecture

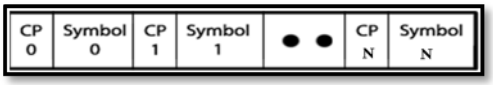


Figure 2. OFDM Frame Format

As receiver and transmitter are physically separated, the receiver to be able to perform an efficient demodulation has to perform frame and carrier synchronization. The first operation defines the starting / ending points of the frame while the latter synchronizes the phase / frequency between transmitter and receiver. Erroneous frame detection is projected into the symbol constellation with a circular rotation, whereas the carrier frequency offset (CFO) causes all the subcarriers to shift and is projected as dispersion in the constellation points. Both ambiguities yield the received signal:

$$r(k) = s(k-\tau)e^{j2\pi\varepsilon k/N} \quad (1)$$

where ε is the normalized CFO, τ is the unknown arrival time of a frame, s(k) is the transmitted signal, N is the number of samples per symbol and k is the sample index of each symbol ranging [0,1023].

IV. SYSTEM GENERATOR FLOW ON SYNCHRONIZATION

The following subsections present the synchronization algorithm divided in three parts.

A. *Estimation of symbol arrival time and carrier frequency offset*

The subsystem presented on this subsection is based on the algorithms developed by Beek [11]. The subsystem created for its purpose and adapted to the symbol pattern on Figure 2 is illustrated in Figure 3. Beek exploits the CP by correlating it with a delayed version of itself. When the repeated pattern is located, a peak is generated in order to detect the frame arrival and the phase between patterns gives the CFO.

The algorithm consists of two main branches. The top one calculates an energy term. While the bottom one calculates the correlation term required for estimating both

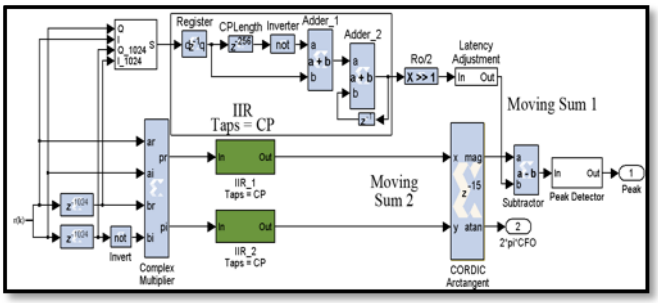


Figure 3. Estimation algorithm architecture

symbol arrival time and phase offset. Equation (2) shows the calculation of the energy term and Equation (3) shows the calculation of the correlation term.

$$ms1 \equiv \frac{\rho}{2}\sum_{k=m}^{m+L-1}\left|r(k)\right|^2 + \left|r(k+N)\right|^2 \quad (2)$$

$$ms2 \equiv \sum_{k=m}^{m+L-1} r(k)r^*(k+N) \quad (3)$$

The factor ρ is the magnitude of the correlation coefficient between *r(k)* and *r(k+N)*; it depends on the signal-to-noise ratio but can be set to 1. Both moving sums were designed using infinite impulse response (IIR) filters. The complex multiplier core present on the System Generator libraries performs multiplications throughout the subsystem. In order to proceed with both estimations, two operations must be performed on the bottom branch, a complex module to create the peak when the CP correlates with its delayed version and an arctangent to calculate the angle between both IQ signals to enable CFO estimation. System Generator provides a CORDIC arctangent reference block that implements a rectangular-to-polar coordinate conversion using a CORDIC algorithm in circular vectoring mode, that given a complex-input <I,Q>, it computes a magnitude and an angle according to (4) and (5), respectively.

$$\left|I,Q\right| = \sqrt{I^2+Q^2} \quad (4)$$

$$ang = 2\pi\varepsilon = \arctan(Q/I) \quad (5)$$

 ISBN: 978-1-61208-231-8

It is assumed that the offset between oscillators is lower than a single subcarrier and so $|\varepsilon| < 1/2$. Reference [13] performs a division to create the necessary peak for frame arrival detection, but such operation in hardware is more expensive and should be avoided. The only difference brought by the difference operation is how the peak is generated, since the argument to be detected will be close to 0 with a subtraction and to 1 with a division. Achieving a theoretical value of 0 when a signal is detected is not a realistic approach since the fixed-point logic used is subject to quantization errors and to contention of bit propagation along the system. The computed angle is only used when the peak is detected, ensuring the CFO is only used if the correlation is complete.

TABLE I. SYSTEM PARAMETERS

System Parameters	
Baseband frequency || Bandwidth	15.36 MHz || 10 MHz
FFT size || CP size	1024 || 256
Modulation	QPSK
Subcarrier separation	15 kHz
Symbol duration (Symbol+CP)	66.66 + 16.66 = 83.32 μs
IF sampling frequency	61.44 MHz
Oscillator frequency	7.68 MHz

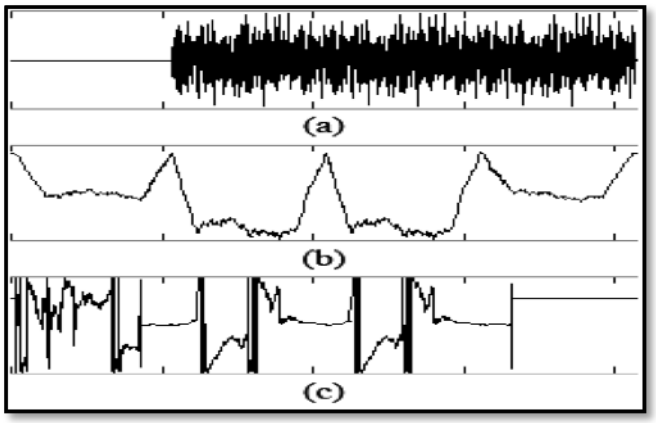


Figure 4. Estimation algorithm results for a frame with 3 OFDM symbols: (a) signal, (b) peak detection and (c) computed angle.

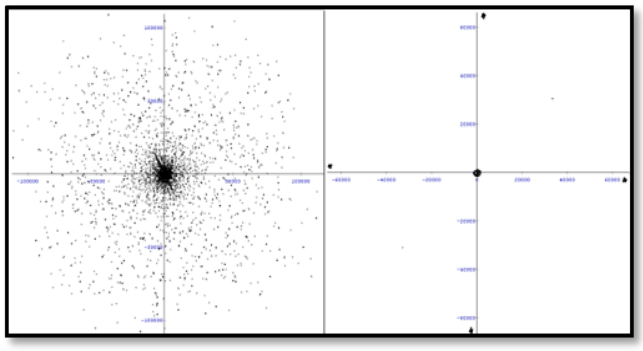


Figure 5. OFDM symbol with a 6 kHz offset between oscillators. Before compensation (left) and after compensation (right).

B. *Data forwarding control*

This subsystem uses the frame detection peak to process the frame in order for each symbol to be processed by the FFT. Unlike a non-deterministic simulation such as the ones ran in Simulink, a FPGA simulation doesn't have the ability to hold the information on its own while the estimations described on the previous subsection are executed. Data must be contained in a memory and forwarded when a condition is met or delayed by a constant value if the process is continuous, which is the case. The processing time required for a peak to be detected and the accurate CFO to be estimated is known, constant and introduced as a delay before the FIFOs. The peak detected on subsection *A* triggers the frame writing into the FIFOs. The CP is not needed anymore so it's not stored. The FFT will require 3*N samples to process each symbol and send it back outside. These amount of samples needs to created given that the symbols stored on the FIFOs are continuous. Reading the data stored on the FIFOs at a sampling rate four times higher as the symbols arrive creates that gap, breaking the frame back into separate symbols.

C. *Carrier frequency offset correction*

Correction of the CFO is achieved with a CORDIC implementing a rotate function [12]. The core rotates the vector (I,Q) by an angle ϕ yielding a new vector (I',Q') such that

$$I'(k) = I(k) \times \cos\phi - Q(k) \times \sin\phi$$
$$Q'(k) = Q(k) \times \cos\phi + I(k) \times \sin\phi \quad (6)$$

where

$$\phi = 2\pi\varepsilon k / N \quad (7)$$

and k is the sample index of each symbol. Taking the angle achieved at subsection *A*, the angle is first divided by N and then accumulated along each symbol nullifying the phase offset along each symbol.

V. TESTBED AND SIMULATIONS

Even though there is not a targeted standard at this point, such implementation can be adapted to several OFDM standards such as 802.11a, WiMAX, 3GPP LTE, among others, given the reconfigurability of the parameters. Xilinx

 ISBN: 978-1-61208-231-8

System Generator for DSP does not allow the user to replace hardware description language (HDL) completely but allows him to focus the attention on the critical parts of the design, i.e., when it comes to managing internal clocks and optimizing paths, HDL is better suited. The design was compiled through hardware co-simulation, a compilation method that allows the user to avoid HDL completely if no front-end is needed.

The targeted model for the simulation was the Xilinx ML605 development board, which contains a Virtex-6 LX240T FPGA and a 4DSP FMC150 FMC daughter card with a dual 14-bit 250 MSPS ADC and a dual 16-bit 800 MSPS DAC.

The tests were performed in a wired-channel and the system was run at a system clock of 61.44 MHz with an IF of 7.68 MHz. The results were obtained using the Xilinx ChipScope Pro tool. Because of the analog front-end present on the testbed, a wrapper must be created with Xilinx ISE Design Suite in order to connect both the system presented here and the daughter card where the DACs/ADCs are present. Table 2 shows the resources used for the full transceiver, without the wrapper.

VI. SIMULATION RESULTS

In Figure 4, a rough estimation of the frame is presented, with a peak being generated at the beginning of each symbol and the respective CFO on the bottom, thus proving an accurate arrival time and CFO estimation of each symbol. It is also possible to perform a frame-based estimation instead of a symbol-based one, but no additional complexity is brought by this change.

Figure 5 proves that OFDM is sensitive to frequency offsets and even though the CORDIC corrects the phase along the symbol, it lacks the ability to compensate for the initial phase present on the oscillator.

VII. CONCLUSION AND FUTURE WORK

A full baseband + IF design was presented focused on the synchronization algorithm. The work presented was performed using Xilinx System Generator for DSP, ChipScope Pro, ISE Design Suite and validated with Matlab.

It is possible to do FPGA simulations with a double floating-point precision, but not all blocks present on the System Generator libraries allow such precision and operations on floating point have a higher resource usage in hardware. Also, the front-end only allows a fixed point precision.

TABLE II. RESOURCE USAGE OF THE FULL SYSTEM

Full system resource usage for Virtex-6		
Parameter	***Used***	***%***
Slices	6662	17
Slice registers	24847	8
Slice LUTs	22059	14
Block RAMs	38	3
DSP48E	141	18

The next step is to direct the work presented here towards a 3GPP LTE MIMO-PHY receiver layer implementation with channel equalization and channel encoding algorithms.

ACKNOWLEDGMENT

The Portuguese projects CROWN, PTDC/EEA-TEL/115828/2009, and CelCop as well as the Mobile Network Research Group (MOBNET) from the Instituto de Telecomunicações in Aveiro supported the work presented on this paper.

REFERENCES

[1] R. W. Chang, “Synthesis of band-limited orthogonal signals for multi-channel data transmission”, Bell System Technical Journal 45, 1966, pp. 1775-1796.

[2] ETS 300 401, “Radio broadcasting systems; Digital Audio Broadcasting (DAB) to mobile, portable and fixed receivers”, ETSI, Feb. 1995.

[3] M. Majó, “Design and implementation of an OFDM-based communication system for the GNU radio platform”, Master Thesis, Dec. 2009.

[4] A. Marwanto, M. A. Sarijari, N. Fisal, S. K. S. Yusof and R. A. Rashid, “Experimental study of OFDM implementation utilizing GNU Radio and USRP – SDR”, Proc. of the IEEE 9th Malaysia International Conference on Communicatons, Dec. 2009, pp. 132-135.

[5] P. Murphy, A. Sabharwal, and B. Aazhang, “Design of WARP: a wireless open-access research platform”, Proc. of the European Signal Processing Conference, Sept. 2006, Article No. 7.

[6] P. Murphy, A. Sabharwal, and B. Aazhang, “On building a cooperative communication system: testbed implementation and first results”, EURASIP Journal on Wireless Communications and Networking, June 2009, doi:10.1155/2009/972739.

[7] J. Garcia and R. Cumplido, “On the design of an FPGA-based OFDM modulator for IEEE 802.11a”, 2nd International Conference on Electrical and Electronics Engineering”, Sept. 2005, pp. 114-117.

[8] E J. Garcia and R. Cumplido, “On the design of an FPGA-based OFDM modulator for IEEE 802.16-2004”, 2005 International Conference on Reconfigurable Computing and FPGAs, 2005, pp. 22-25.

[9] A. Goldsmith, “Wireless Communications”, Cambridge University Press, 2005.

[10] Xilinx Inc., “System Generator for DSP user guide”, http://www.xilinx.com/support/documentation/sw_manuals/xilinx13_3/sysgen_gs.pdf, Release 13.3, Oct. 2011 [retrieved: Nov., 2012].

[11] J. van de Beek, M. Sandell, and P. O. Börjesson, “ML estimation of time and frequency offset in OFDM systems”, IEEE Transactions on Signal Processing, vol. 45, no. 7, July 1997

[12] Xilinx Inc., “DS249 LogiCORE IP CORDIC v4.0”, http://www.xilinx.com/support/documentation/ip_documentation/cordic_ds249.pdf, March 2011 [retrieved: Nov., 2012].

[13] O. Font-Bach, N. Bartzoudis, A. Pascual-Iserte, and D. L. Bueno, “A real-time MIMO-OFDM mobile WiMAX receiver: Architecture, design and FPGA implementation”, Computer Networks, 55 (16), pp. 3634-3647, 2011.

[14] Xilinx Inc., “System Generator for DSP reference guide”, http://www.xilinx.com/support/documentation/sw_manuals/xilinx13_3/sysgen_ref.pdf, Release 13.3, Oct. 2011 [retrieved: Nov.,2012

 ISBN: 978-1-61208-231-8

Uplink Throughput Improvement at Cell Edge using Multipath TCP in Overlaid Mobile WiMAX/WiFi Networks

Miguel Angel Patiño González, Takeshi Higashino, and Minoru Okada
Graduate School of Information Science
Nara Institute of Science and Technology
630-0192 Ikoma-shi, Japan
{*miguel-p, higa, mokada*}*@is.naist.jp*

***Abstract*—Recently, many laptops, smartphones and tablets are equipped with several broadband wireless interfaces, such as WiFi and Mobile WiMAX. However, the current Transport Control Protocol (TCP) only allows a single interface to be active at any moment, while the remaining ones are not used. Multipath TCP (MPTCP) is a proposed extension to standard TCP, which aims to exploit the availability of such multiple interfaces. This multipath capability is of great importance for current and future communication systems. In this work, we study the potential of MPTCP for improving uplink throughput at the WiMAX cell edge by dynamic data offloading to WiFi. To this end, we conducted measurements on real Mobile WiMAX/WiFi networks. The results show that MPTCP can significantly improve the uplink throughput of Mobile WiMAX users and also reduce the round-trip time (RTT).**

***Keywords*-Mobile WiMAX; cell edge; MPTCP.**

I. INTRODUCTION

The Internet is becoming mobile, as traditional voice-oriented cellular networks introduce enormous advances in data transmission capabilities. Mobile data traffic is growing very fast, with an 18-fold increase forecast between 2011-2016 [1]. Thus, Mobile Service Operators need to solve the critical problem of the throughput performance in their mobile networks. As more users connect to the network, the congestion levels increase accordingly. Furthermore, the popularity of devices with multiple interfaces introduces a new end-to-end communication paradigm. The conventional TCP/IP protocol stack assumes that end-systems communicate with each other by using a single connection point, i.e.,one IP address. However, the availability of multiple interfaces (and multiple IP addresses) within a single device enables it to transmit and receive through diverse paths over the Internet. Therefore, it is desirable to have the capability of using more than one interface at any time.

WiMAX has emerged as an important technology for Wireless Broadband communications [2]. Many telecom operators around the world have adopted it as an alternative to wired technologies. This technology belongs to the IEEE 802.16 family and has two main variants: 802.16d (Fixed Access WiMAX), and 802.16e (Mobile WiMAX). At the Physical Layer, Mobile WiMAX employs Orthogonal Frequency Division Multiplexing (OFDM), while the available modulation schemes are BPSK, QPSK, 16-QAM and 64-QAM. It also implements an Adaptive Modulation and Coding (AMC) functionality, which enables dynamic adjustment of the transmission profile depending upon the current radio signal condition. According to [6], the average throughput per sector ranges between 4-15 Mbps for uplink, and 9-28 Mbps for downlink, using TDD with several frequency bandwidth between 10-20 MHz.

Additionally, it is a very common practice to assign more transmission channels to the downlink than the uplink, with typical ratios of 2:1 and 3:2. Thus, in most cases the uplink has lower capacity than the downlink. This is an important fact to consider, because nowadays a growing number of users are generating traffic (uploading) from their mobile devices to the Internet, instead of receiving traffic (downloading) from it. These applications range from interactive video conferencing, remote video surveillance, and regular uploading of large files. Therefore, it is important to explore new alternatives for improving the uplink throughput.

In this paper, we explore the Multipath Transmission approach. The fundamental idea is to transmit over more than one path towards the final destination. As mentioned previously, mobile devices with more than one interface are already available nowadays, thus enabling the implementation of such Multipath scheme. A promising new protocol suitable for this purpose is Multipath TCP (MPTCP) [3], and it is the choice for our study.

The rest of the paper is organized as follows. In Section II, we describe related work. Next, in Section III we introduce the basics of MPTCP. In Section IV we present the experimental setup. Then, in Section V we analyze the measurement results. Section VI presents a brief discussion of the results. Finally, Section VII concludes the article.

II. RELATED WORK

Several works on multipath transmission have been presented. Iyengar *et al* [9] presented a scheme called Concurrent Multipath Transfer (CMT), based on the Stream Control Transmission Protocol (SCTP), which added the capability of transmitting over multiple interfaces. Later, Koh *et al* [10], extended SCTP to support traffic handover

 ISBN: 978-1-61208-231-8

among interfaces, best suited for mobile environments where new IP addresses are possibly assigned while moving around an area. Although these studies showed interesting results, SCTP is not widely adopted in the current Internet.

Multimedia streaming via Transmission Control Protocol (TCP) has been deployed successfully over recent years. Thus, an extended multipath capability for TCP streaming has also been proposed by Wang *et al* [11]. The authors proved the feasibility of this approach for practical scenarios.

The use of WiFi for offloading traffic from cellular networks has also been proposed in earlier works. Balasubramanian *et al* [13] studied the feasibility of augmenting Mobile 3G using WiFi. They analyzed measurements made in three cities from a moving vehicle. Positions of the WiFi access points were recorded and used by an algorithm for determining their proximity at a given moment. After implementing their solution called Waffler, they determined a reduction of 45% in 3G usage. However, they did not consider simultaneous interface usage, since their approach is based on a single interface opportunistic scheme.

An experimental study on the throughput gains when using a new protocol called Multipath TCP (MPTCP) was presented by Raiciu *et al* [12]. The authors proved the functionality of MPTCP while moving inside a building with 3G and WiFi coverage. They moved from floor to floor while measuring the corresponding variability in the signal levels from 3G and WiFi. After comparing the measurements against an optimal TCP scheme, the gains obtained with MPTCP were at least 12%. They also simulated walking and driving scenarios, reporting gains ranging between 50-100%. However, the results showed only downlink performance, and details about radio signal conditions were not specified.

In our work, we have chosen MPTCP, due to its compatibility with current Internet. We study the uplink performance, which was not considered in previous studies. Also, we focus on the most challenging area of any wireless system, the cell edge, which was also not considered.

III. MULTIPATH TCP (MPTCP)

In current Internet technology, Transmission Control Protocol (TCP) is one of the most important transmission protocols. It has reached maturity over the years and most of the available services use it. However, it was originally designed for managing communications over a single path between two end-hosts. At any time, TCP uses only one interface, regardless of the total available interfaces. This fact limits the potential of the increasingly popular multi-interface mobile devices, resulting in their under-utilization. Thus, it is desirable to have more flexibility in the selection of transmission resources.

Multipath TCP (MPTCP) is an extension to conventional TCP, which aims to leverage the concurrent use of multiple interfaces within a single device. Currently, it is being standardized by an active working group at IETF [7]. The most important features of MPTCP when compared to conventional TCP are:

- Connection Reliability: enables connection recovery when one or more links become unavailable, by dynamically selecting an appropriate interface.
- Throughput Improvement: enables bandwidth aggregation by simultaneous use of multiple interfaces.

Moreover, a very important advantage of MPTCP is its compatibility with current Internet architecture and services. It does not require changes either to existing infrastructure or applications. Therefore, it can be used transparently from both the user and network point of view.

The MPTCP working group also pays considerable attention to wireless scenarios similar to the one described in our work, as they envisage the necessity of wireless networks converging [8].

IV. EXPERIMENTAL SETUP

In this study, we conducted field measurements on real networks within a university campus. Specifically, we used a commercial Mobile WiMAX network and the campus WiFi. Our objective was to investigate the effects of MPTCP use on WiMAX uplink throughput in a overlaid WiMAX/WiFi scenario. In particular, we focused on cases with poor radio signal conditions, with power levels equivalent to those at a cell edge. The reason for choosing this particular case was that it represents the most challenging environment for a mobile device.

Figure 1 shows the tested scenario. The Mobile WiMAX Base Station was located on the rooftop of a five-story building, and it is referred to as BS. The WiFi network is based on 802.11g (2.4 GHz), providing good coverage within the university campus. Measurement locations are indicated by points A and B. The distances BS-A and BS-B are approximately 370 and 280 meters, respectively. The Mobile WiMAX antenna was located at 30 meters high, transmitting at 20 Watts. The frequency band was 2.62 GHz, with channel bandwidth of 10 MHz. The system was operating in TDD mode.

Location A has better WiMAX RSSI and higher CINR. When checking the relative positions of A and B in Figure 1, it is important to clarify that location A has a better radio condition for WiMAX because it has more favorable Line-Of-Sight (LOS) to BS, even though it is farther away. On the other hand, location B is closer to the BS, but its LOS is obstructed by a building, which introduce additional degradation to the link quality. On the other hand, WiFi RSSI values show the opposite behavior, being worse at A than B. Location A is outside the campus and far away from the WiFi Access Point (AP), while location B is within the campus, close to the AP.

The measuring equipment was a laptop equipped with a WiFi interface and a Mobile WiMAX Router connected to it through an USB port. In the experiments, we measured

 ISBN: 978-1-61208-231-8

Figure 1. Base Station and Measurement Locations

Table I
RADIO SIGNAL CONDITIONS

Location	WiMAX RSSI (dBm)	WiMAX CINR (dB)	WiFi RSSI (dBm)
A	-75	16	-90
B	-81	10	-65

the uplink throughput at locations A and B. In both cases, WiMAX had low signal strength, while WiFi radio condition was poor at one location and good at the other. The average values are shown in Table I.

To test the MPTCP functionality, we installed the publicly available MPTCP Implementation developed by Barré et al [15]. Our testing laptop runs the Linux Kernel version 3.2.0 along with the mentioned patch.

We used the networking tool *iperf* to conduct the measurements [4]. Then, we tested the connection quality to the Kernel implementers website located in Belgium, which is also running MPTCP [5]. This was deliberate, to confirm the functionality when sending traffic across the Internet.

The measurements were conducted over two weeks, twice a day, at 11 AM and 16 PM. Both sessions lasted 1 hour, where five-minute long flows were transmitted.

V. EVALUATION

In this section we introduce our measurement results. Our objective is to investigate how MPTCP affects uplink performance in an overlaid WiMAX/WiFi scenario. We analyze not only the absolute values of the throughput, but also use the Coefficient of Variation (CV) parameter to get a normalized comparison value. Thus, we analyze the throughput variability by using Eq. 1:

$$CV = \frac{StdevThp}{AvgThp} \quad (1)$$

where $StdevThp$ is the Standard Deviation and $AvgThp$ is the Average of measured Throughput. Low CV indicates that most values lie close to the average, whereas high CV suggests values that are distant from the average, i.e., more dispersed values.

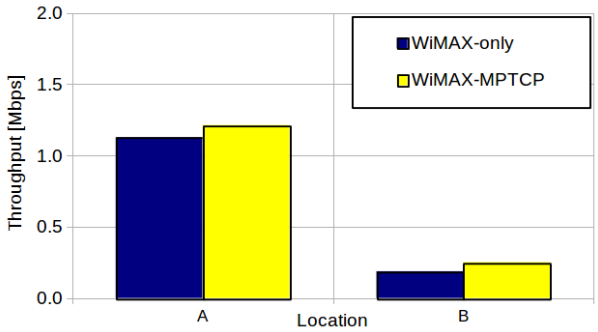


Figure 2. Mobile WiMAX Uplink Throughput

A. WiMAX-only uplink throughput

Initially, we measured the WiMAX-only uplink behavior at locations A and B. We wanted to compare the difference in the throughput at both locations, to determine the initial reference values. The results are shown in Figure 2. While at location A, the average throughput was 1.1 Mbps, at location B it was only 0.18 Mbps. The difference between the throughput values at A and B is due to the good LOS in BS-A path, as well as the shadowing effect by the building in the BS-B path, which introduces about 6 dB of attenuation.

Next, we enabled MPTCP transmission and used WiMAX and WiFi simultaneously. The WiMAX component of the total traffic over MPTCP was 1.2 Mbps at A and 0.25 Mbps at B. In practical terms, these values can be considered nearly equal to the previous WiMAX-only values. Thus, MPTCP was able to fully use the WiMAX link capacity at both locations.

Another interesting characteristic to investigate is the Throughput Variability. To this end, we used the Coefficient of Variation (CV) defined in Eq. 1. The results are shown in Figure 3. The WiMAX-only case showed a CV increase of 0.13, from 0.29 to 0.42 at locations A and B, which indicates that the throughput fluctuation around the average increased slightly. However, when MPTCP was enabled, the CV increased about 1.27, from 0.36 to 1.63 at A and B, much more than the previous value. This means that there are relatively high values, which are distant from the average and appear in a sporadic way during the observation time. In other words, this behavior shows that the WiMAX interface increased its traffic only occasionally. If we take this to the limit, WiMAX will not transmit any traffic at all, and WiFi will carry the total traffic, practically resulting in a vertical handover. However, this is not allowed under normal operation, because MPTCP needs to keep some traffic on each interface, to probe the links and make appropriate traffic distribution decisions.

B. MPTCP total uplink throughput

Here, we consider the Total uplink Throughput result when using WiMAX and WiFi simultaneously. Figure 4

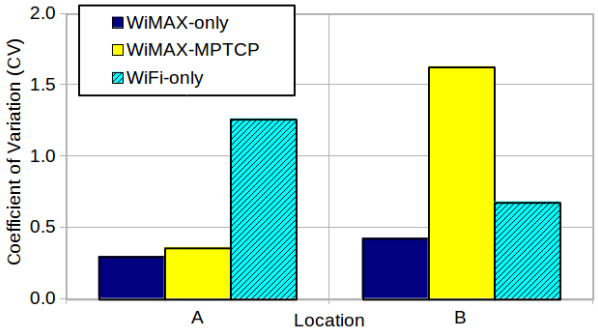


Figure 3. Coefficient of Variation

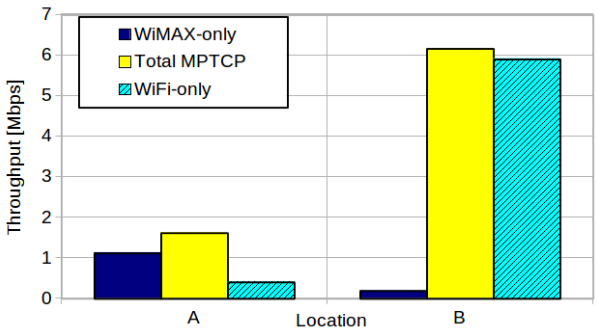
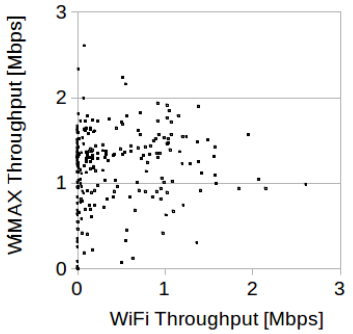
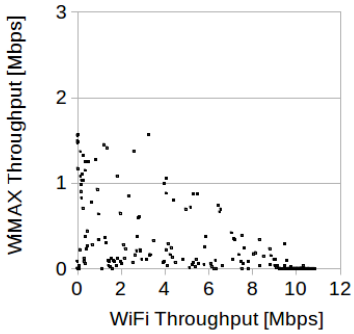


Figure 4. Total Throughput using MPTCP



(a) Location A



(b) Location B

Figure 5. Traffic Distribution over WiMAX and WiFi

shows the measured values. We compared this result to the WiMAX-only case from Figure 2. At location A, the throughput increased from 1.1 Mbps to 1.6 Mbps, or about +33%. Considering that, at this location, WiFi is operating at nearly its cutoff signal level, this increase indicates the advantage of using Multipath transmission. The throughput increase was much more abrupt at location B, from 0.2 Mbps to 6.1 Mbps. The reason for such a huge increase was the high-speed WiFi, which became prevalent. In this case, the resulting throughput aggregation had more similarity to a vertical handover from WiMAX to WiFi.

Overall, the aggregation capability of MPTCP showed important gains on the user's total throughput when compared to using only WiMAX. Moreover, the WiMAX cell capacity is indirectly increased because less WiMAX resources are used, since a portion of the traffic is sent over WiFi.

C. Traffic distribution among interfaces

One of the MPTCP design objectives is to distribute traffic fairly among available interfaces. In Figure 5 we show the measured traffic distribution over WiMAX and WiFi at locations A and B.

At location A, we verified that WiMAX gets more throughput than WiFi about 88% of the time. This was determined by observing the samples above the 45 degree line. The traffic distribution for location B was nearly the opposite, because WiFi gets more throughput than WiMAX about 86% of the time, which was an expected value due to the good signal strength of WiFi. These values are located below the 45 degree line.

The traffic distribution over real networks strongly depends on the current network congestion and wireless link quality. In our scenario, the traffic distribution should be ideally 50-50% among WiMAX and WiFi interfaces. However, due to asymmetries in terms of bandwidth capacity and wireless connection quality, the distribution was expected to be asymmetric too. On the one hand, the WiFi network has much more available bandwidth than WiMAX, and it was prevalent when it had good wireless link conditions. On the other hand, when WiFi quality degraded, it became more unstable.

D. Round-trip time

Another important parameter is the round-trip time (RTT) between end-hosts. This parameter is especially important for many real-time applications such as video-conferencing and Voice over IP (VoIP) running on TCP. The results are shown in Figure 6. The WiMAX-only transmission suffers from a large RTT at both locations. While the values at Location A reached about 843 ms, the values at Location B reached about 1500 ms.

 ISBN: 978-1-61208-231-8

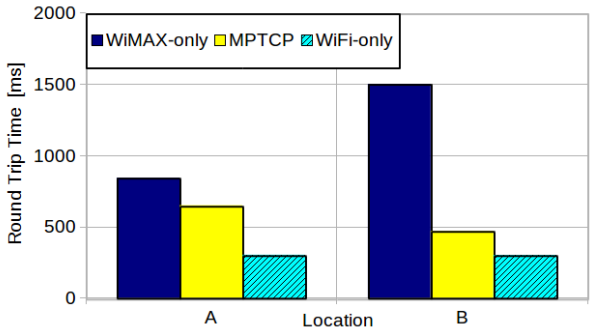


Figure 6. Round-trip Time (RTT)

On the other hand, the WiFi RTT values are much lower and they are consistently around 300 ms at both locations. As expected, for MPTCP we found values in between WiMAX and WiFi. At location A, an RTT of around 650 ms was observed, which represents a reduction of about 23% from WiMAX-only, thanks to the collaboration of WiFi. The RTT at location B was around 470 ms, a reduction of almost 70%, due to the high dominance of WiFi. Hence, these improvements also demonstrate the advantage of introducing MPTCP in this scenario, reducing the RTT values by considerable percentages.

VI. Discussion

Although using MPTCP is advantageous in overlaid networks, we should consider some factors affecting its performance. One of them is the IP configuration procedure. Before transmitting any useful data, the mobile device needs to first be associated with the access points and authenticated. Only then is the user granted access to the network. This procedure takes about 4 to 5 seconds to complete, which is relatively slow. Additionally, the routing configuration is lost whenever the device goes out of range from Mobile WiMAX or WiFi. Thus, whenever the connection is re-established, the routing information is not complete and the procedure needs to be performed again, introducing even more delay. We alleviated this issue by creating monitoring scripts, which reconfigured the routing tables in the events of connection/disconnection to the access point. However, fully automatic configuration will be necessary.

Another effect is caused by TCP itself, since it takes an additional 3 to 5 seconds to reach a steady throughput level after TCP flow initiation. This characteristic also prevents users from getting faster access to the network capacity, and could have a considerable impact especially in high-mobility environments, which we did not cover in this paper.

For more complex environments, where multiple radio bases and access points co-exist, it is important to identify and properly choose the most advantageous connections. Factors affecting this decision could be technical, e.g., signal levels, bandwidth, delay, and jitter, or financial, e.g., cost, or limited data transmission. MPTCP can already detect congested networks and move the traffic away from them [17], but an additional consideration of the current radio signal conditions could be interesting for evaluating the connection quality.

Interactive applications can also benefit from MPTCP. Although further evaluation is needed, we have conducted preliminary tests showing that it is possible to get packet losses below 0.5% when using Skype. MPTCP will be especially useful with weak radio signal conditions, where the connection is unreliable and subject to rather frequent disconnection events. By having an additional communication path, the impact of these disconnection events could be reduced.

We measured uplink-only throughput because previous works did not show it. It should be recalled that uplink resources are more scarce. Also, it may be affected by downlink traffic.

VII. Conclusion and Future Work

In this work, we conducted an experimental study of the uplink throughput when using Multipath TCP (MPTCP) in a overlaid Mobile WiMAX/WiFi scenario. Our interest was to verify the potential benefits of a multipath protocol such as MPTCP. In particular, we focused on cases of low WiMAX signal levels, with good WiFi at one location and poor at another. First, we observed a minimum of 33% increase in the achieved throughput, even when the WiFi was near its signal cutoff level. Second, we studied the variability of throughput by introducing the Coefficient of Variation parameter defined as the ratio between the Standard Deviation and the Average Throughput. The main finding was that the WiMAX interface achieved higher throughput only in a sporadic way when WiFi was prevalent. The WiMAX interface was not pushed to its maximum capacity all of the time. Thus, the system behaved as if WiFi had received some priority, effectively reducing the load on the WiMAX network. Third, we analyzed the relative traffic distribution over both interfaces. When the WiFi signal condition was better than WiMAX, it achieved higher throughput 86% of the time. However, when WiMAX was better than WiFi, it had higher throughput 88% of the time. Also, the RTT values showed a reduction of at least 23%, which is very important for real-time applications.

The results demonstrated that multipath protocols, such as MPTCP, are a very interesting option for improving uplink throughput near the cell edge of Mobile WiMAX.

As a future work, it is interesting to explore further considerations for the practical use of MPTCP in mobile networks. We are customizing a Mobile WiMAX/WiFi testbed for the study of MPTCP performance under different network parameters, such as backhaul and WiMAX channel bandwidth, WiFi AP load, among others.

 ISBN: 978-1-61208-231-8

REFERENCES

[1] Cisco Systems. Visual Networking Index 2011-2016.

[2] www.wimaxforum.org 2012-09-24

[3] http://datatracker.ietf.org/wg/mptcp/charter 2012-09-24

[4] http://sourceforge.net/projects/iperf 2012-09-24

[5] http://mptcp.info.ucl.ac.be 2012-09-24

[6] WiMAX Forum. WiMAX, HSPA+, and LTE: A comparative analysis, Nov. 2009.

[7] A. Ford, C. Raiciu, M. Handley, and O. Bonaventure. TCP Extensions for Multipath Operation with Multiple Addresses. *draft-ietf-mptcp-multiaddressed-06*, IETF. Jan. 2012.

[8] G. Hampel, T. Klein. MPTCP Proxies and Anchors. *draft-hampel-mptcp-proxies-anchors-00*, IETF Feb. 2012.

[9] J. Iyengar, P. Amer, and R. Stewart. Concurrent Multipath Transfer using SCTP Multihoming over Independent End-to-End Paths. In *IEEE/ACM Transactions on Networking, 14(5): pp. 951-964*, 2006.

[10] S. J. Koh, M. J. Chang, and M. Lee. mSCTP for Soft Handover in Transport Layer. In *Communications Letters, IEEE, 8(3): pp. 189-191*, Mar. 2004.

[11] B. Wang, W. Wei, Z. Guo, and D. Towsley. Multipath Live Streaming via TCP: Scheme, Performance and Benefits. In *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMCCAP)*, 2009.

[12] C. Raiciu, D. Niculescu, M. Bagnulo, and M. Handley. Opportunistic mobility with Multipath TCP. In *ACM Workshop on MobiArch, pp. 7-12*, 2011.

[13] A. Balasubramanian, R. Mahajan, and A. Venkataramani. Augmenting Mobile 3G using WiFi. In *ACM Mobisys'10*, 2010.

[14] D. Kim, H. Cai, M. Na, and S. Choi. Performance measurement over Mobile WiMAX/IEEE 802.16e network. In *IEEE World of Wireless, Mobile and Multimedia Networks, WoWMoM 2008, pp. 1-8*, June 2008.

[15] S. Barré, C. Paasch, and O. Bonaventure. Multipath TCP: From Theory to Practice. In *IFIP Networking*, May 2011.

[16] S. Barré, O. Bonaventure, C. Raiciu, and M. Handley. Experimenting with Multipath TCP. In *ACM SIGCOMM'10*, Sep. 2010.

[17] C. Raiciu, D. Wischik, and M. Handley. Practical Congestion Control for Multipath Transport Protocols. *UCL Technical Report*, 2010.

 ISBN: 978-1-61208-231-8

PRIPAY: A Privacy Preserving Architecture for Secure Micropayments

Christoforos Ntantogian, Dimitris Gkikakis, Christos Xenakis
Department of Digital Systems
University of Piraeus
Piraeus, Greece
{dadoyan, dimgkik, xenakis}@unipi.gr

***Abstract*—This paper proposes a privacy preserving architecture, called PRIPAY, which enables micropayments and financial transactions through mobile/wireless operators (2G, 3G, WLANs, 4G, etc.) in a secure and efficient manner. It enables the operator to generate and assign a different pseudonym to each requesting mobile user, equipped with a mobile station (MS), every time it wishes to access a remote Merchant or Service Provider, achieving anonymity and unlinkability. PRIPAY hides the real identity of MS from remote Merchants or Service Providers; but, at the same time it allows the operator to track the MS's activities achieving traceability. It utilizes the established trust relationships between mobile users and networks operators, and employs public key cryptography to ensure authenticity, integrity and confidentiality of the assigned pseudonyms. Apart from privacy, PRIPAY constitutes an efficient micropayment solution that enables the operator to aggregate and charge all the user's micropayments during a charging time period (i.e., monthly) within its mobile telephone bill. It is compatible with the employed technologies and minimizes the required typing and configuration effort by mobile users on the reduced-sized smartphones' screens, facilitating m-commerce.**

Keywords-micropayments; privacy; mobile operators; trusted third party.

I. INTRODUCTION

Due to the proliferation of mobile devices, web access by people on the move using their smart phones or tablets is likely to exceed web access from desktop computers within the next years [1]. As the technological capabilities of these devices are increasing, new services are also emerging. For instance, location based services (e.g., geosocial networking, proximity based recommendations, resource tracking, location-based mobile payments, etc.) are expected to flourish, since mobile devices are integrating Global Positioning System (GPS) [2] technology allowing location tracking.

This trend creates a favorable environment for mobile commerce (m-commerce) [3] to emerge and become a profitable market. However, for the proliferation of m-commerce two major issues need to be addressed. The first has to do with the fact that m-commerce poses various privacy threats, including behavioral profiling, tracking of money spent and visited websites, etc. These have also been acknowledged in the EU Directives [4], which identify specific privacy requirements. The second issue is that m-commerce, usually, involves micropayments, which are financial transactions with small or very small amount of money. In cases that the fixed processing cost is greater than the monetary amount of the transaction itself, micropayments become inefficient for the provided goods or services and the involved merchants or service providers (MorSPs) cannot develop their businesses. To overcome this fundamental limitation, new purchase and billing approaches are required [5].

An elegant solution that simultaneously addresses privacy and micropayment requirements is to allow mobile/wireless operators to act as trusted third parties (TTP) between the mobile/wireless subscribers equipped with mobile stations (MSs) and MorSPs. Subscribers already trust operators to maintain and process sensitive information that refer to them, including communication and contacts information, locations, service preferences, billing data, etc. For this reason, operators are obliged to follow specific security procedures and policies when capture, record, process, store and destroy such information. On the other hand, MorSPs are willing to trust mobile/wireless operators in order to charge them for the goods and services that MorSPs offer to their subscribers, ensuring micropayments. This is also strengthen by two facts: a) MorSPs are already subscribers of the mobile/wireless operators and, thus, they have already signed contracts or service level agreements between them; and b) the penetration of mobile/wireless subscriptions is very high, higher than the fixed internet counterpart, which means that mobile/wireless subscribers constitute a big candidate market for e-commence and e-services.

Driven by this observation, this paper proposes a privacy preserving architecture that enables micropayments or any other kind of financial transactions, through mobile/wireless operators in a secure and efficient manner. The proposed architecture, called PRIPAY, introduces a new entity to the mobile/wireless network, called pseudonym provider (PSP), which enables the operator to generate and assign to each requesting MS a different pseudonym, every time MS wishes to have access to a MorSP, achieving anonymity and unlinkability [6]. To efficiently verify that a generated pseudonym has not been previously assigned, a PSP uses a data structure based on bloom filters [7] to store the allocated pseudonyms. PRIPAY hides the real identity of an MS from a remote MorSPs, but, at the same time it allows the operator to track the MS's activities achieving traceability. Moreover, it includes a pseudonym assignment protocol that uses public key cryptography to ensure authenticity, integrity and

 ISBN: 978-1-61208-231-8

confidentiality of the assigned pseudonyms. Apart from privacy, PRIPAY constitutes an efficient micropayment solution that enables the operator to aggregate and charge all the subscriber's micropayment/financial transactions during a charging time period (CTP) (i.e., monthly) within its mobile telephone bill. It can be easily installed in the existing network infrastructure, since it is compatible with the employed technologies. Finally, it minimizes the required typing and configuration effort by mobile users on the reduced-sized smartphones' screens, facilitating m-commerce.

The rest of the paper is structured as follows. In Section 2, the proposed PRIPAY architecture is presented by analyzing its deployment in a representative networking scenario. The basic functionality such as the pseudonym generation and the pseudonym assignment protocol are also elaborated. Section 3 evaluates PRIPAY. Finally, Section 4 includes the related work, while Section 5 contains the conclusions.

II. THE PRIPAY ARCHITECTURE AND DEPLOYMENT

The proposed PRIPAY architecture can be mounted and operate in the most prominent mobile (i.e., 2G, 3G and 4G) and wireless technologies including, General Packet Radio Services (GPRS), Universal Mobile Telecommunication System (UMTS), Wireless Local Area Networks (WLAN), Worldwide Interoperability for Microwave Access (WiMax), and 3G-WLANs integrated networks. In this paper, we describe and analyze the deployment of PRIPAY in a 3G-WLAN integrated network [8], which is a representative scenario of the candidate technologies on which PRIPAY can be deployed (see Figure 1).

A. Network Architecture and Required Enhancments

The 3G part of the integrated 3G-WLAN network [8] architecture mainly includes: a) the Radio Network Controller (RNC) that is responsible for the radio resource management and controls the wireless transceivers (Node Bs); b) the Serving GPRS Support Node (SGSN) that undertakes packet routing and transfer, mobility management, location management and logical link management; c) the Gateway GPRS Support Node (GGSN) which is responsible for the interworking between 3G and external networks (e.g., Internet), as well as for IP allocation to MSs; and d) the Home Location Register/Home Subscriber Server (HLR/HSS) which is a database that contains subscription, authentication and billing information for mobile users. On the other side, the WLAN technology that participates in the 3G-WLAN architecture consists of: i) the Authentication Authorization and Accounting (AAA) server which retrieves subscription and authentication information from the HLR/HSS and validates the authentication credentials that MSs provide; ii) the Packet Data Gateway (PDG) which provides access to external networks; and c) the WLAN Gateway that connects WLAN access points with the AAA server and PDG.

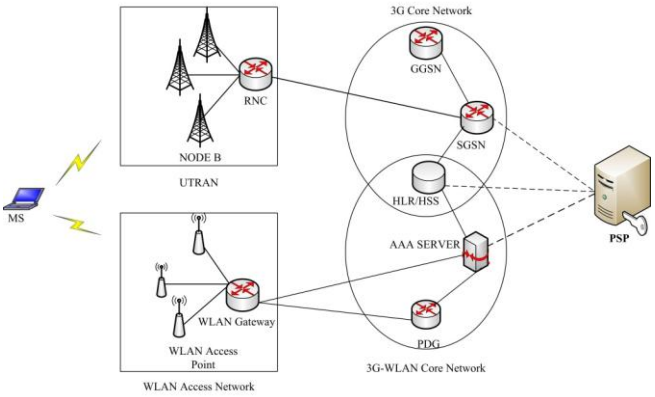


Figure 1. PRIPAY deployment in a 3G-WLAN integrated network

The key functional component of PRIPAY is PSP, which generates and assigns pseudonyms to the requesting MSs in a secure and efficient manner. In the considered 3G-WALN network architecture, PSP is placed within the core network of the mobile/wireless operator, which is deployed on a private/controlled network environment interconnected to the public Internet. This network and the included entities are protected from the security threats of the public Internet by establishing specific security measures (e.g., Firewalls, Intrusion Detection Systems, Virtual Private Networks, etc.) and following definite security policies.

PSP interfaces and interacts with SGSN and the AAA server, in order to make available the PRIPAY functionality and the provided services to the underlying networks and their subscribers. SGSN and the AAA server play similar roles in managing mobile/wireless subscribers in an integrated 3G-WLAN network architecture, where the subscribers wish to have access to external networks and services. PSP also interfaces to HLR/HSS, which records every assigned pseudonym to a specific subscriber for accessing an explicit remote MorSP. The interfaces between PSP and the core network components (i.e., SGSN, HLR/HSS and the AAA server) are based on the Mobile Application Part (MAP) of the SS7 protocol stack, where some new message exchanges need to be developed, as shown in Section II.C. As the three network nodes already execute the MAP protocol, the required enhancements have minimum impact on the existing infrastructure.

Except for the enhancements on the interfaces, PRIPAY requires some extensions to the existing HLR/HSS database scheme. More specifically, for each subscribed user the new extended scheme will include a list of pseudonyms that have been assigned to it, together with the MorSP that each pseudonym has been issued as well as the time of assignment. These entries will be updated by PSP when a new pseudonym is generated, as mentioned below. Finally, the operation of PRIPAY requires from each of the involved parties (i.e., mobile/wireless operators and the participating MoSPs) to possess a valid public key certificate.

B. Pseudonym Generation and Assignment

An essential requirement of PRIPAY is that within a particular CTP a specific pseudonym should be used only

 ISBN: 978-1-61208-231-8

once, and only from one MS. In this way, the architecture achieves unlinkability between different actions of the same MS, as well as ensures secure charging in cases of micropayment or financial transactions. For this reason, PSP maintains a bloom filter to keep record of all the generated pseudonyms and efficiently check whether a pseudonym has been previously assigned. As bloom filters have been applied and analyzed extensively in many networking applications [8], we highlight only the basic functionality of them.

A bloom filter is a data structure for representing a set S $=\{x_1, x_2, x_3,\ldots,x_n\}$ of n elements by an array of m bits. Initially, all bits of the array are set to 0. A bloom filter uses k independent hash functions $h_1, h_2, h_3,\ldots,h_k$ with range $\{1,2,3,\ldots,m\}$. To insert a new element x in the set S, the bits $h_i(x)$ are set to 1 for $1 \leq i \leq k$. To check if an element y belongs to S, we check whether all $h_i(y)$ are set to 1. If not, then y is not a member of S. If all $h_i(y)$ are set to 1, it is assumed that y is in S. However, this may be wrong with some probability *p*, due to collusions of the hash functions employed. Hence, a bloom filter may yield a false positive, where it outputs that an element x is in S, even though it is not. Figure 2 depicts a bloom filter with k=3 hash functions that inserts the x_1 and x_2 elements and checks whether the y_1 and y_2 elements belong to this set. The key advantage of bloom filters lies in the fact that the time needed either to add new elements or to check whether an element is in the set, is a fixed constant O(k) (k is the number of hash functions employed), independent of the number of elements already in the set.

In PRIPAY, the assigned pseudonyms represent the set of elements S of the bloom filter. When a new pseudonym is generated, PSP uses the bloom filter to efficiently check whether the pseudonym is already in the set. If it is (i.e., this means that the pseudonym has been already assigned to an MS), PSP generates a new one, and, then, checks whether the new pseudonym is included in the set. This procedure continues until PSP generates a pseudonym that is not included in the bloom filter (i.e., means that it has not been assigned yet). Next, PSP inserts this pseudonym into the bloom filter (i.e., sets the appropriate locations in the array of the bloom filter equal to 1). The operation of PRIPAY continues until its runtime reaches the predefined CTP value. Then, the operator processes the PRIPAY records included in HLR/HSS (i.e., International Mobile Subscriber Identities - IMSIs, pseudonymous, accessed MorSP, access time) and provides charges to the subscribers involved in micropayments or financial transactions. The charges are completed and verified by using the related expenses that the accessed MorSPs have requested from the operator. The recorded and processed data can be stored in a secure place for a certain period of time (i.e., one or two years), according to the operator's policies and the government regulations. Having finished the processing and storing of PRIPAY records, HLR/HSS resets the assigned pseudonyms (and the related information), PSP initializes the employed bloom filter by setting all bits with 0s and both of them continue operation for another CTP.

As mentioned previously, the main drawback of a bloom filter is the occurrence of false positives, where it erroneously indicates that an element belongs to the considered set, but, actually, it does not. However, false positives do not have any impact on the functionality of PRIPAY and impose some minor effects on its performance. More specifically, in case of a false positive, PSP aborts a fresh pseudonym, generates a new one and checks again if it is included in the maintained bloom filter. The cost of this operation is O(k), which is constant and does not affect the performance of the architecture. In addition, in every CTP, PRIPAY resets the bloom filter reducing the occurrence of false positives.

The probability *p* of a false positive in a bloom filter is given by the formula $p \approx (1 - e^{-kn/m})^k$, where k is the number of hash functions, m is the number of bits in the array of the bloom filter, and n is the number of elements in the bloom filter. It is evident that the probability of a false positive *p* reduces when the number of bits m is increased or the number of elements n is reduced. Moreover, the optimal value of k is given by k= ln2(m/n). In PRIPAY, the number of elements n (i.e., the assigned pseudonyms) is equal to the total number X of the privacy service requests, performed in a CTP. To estimate the storage cost of a bloom filter implementation (i.e., the number of bits m) in the PRIPAY architecture, we consider three representative values of X: i) $X= 10^4$, ii) $X= 10^5$, iii) $X= 10^6$. In all cases, we keep an optimal value of k= ln2(m/n) = 17 and a small value *p* (i.e., $p=10^{-5}$) to minimize false positives. As shown in Table I, the storage cost is very low in all three cases and even for $X=10^6$, the storage cost is approximately 3MB, which is a negligible cost. Based on this finding, it can be inferred that if the value of X increases (e.g., due to an increase of the total number of subscribers or of the privacy service requests), the mobile operators can easily increase the storage cost to preserve the probability of false positives very low.

TABLE I. MEAN NUMBER OF PRIVACY REQUESTS IN A CTP VS. STORAGE COST (K=17 AND P=10^{-5})

Number of Privacy Requests X	Storage Costs
10^4	29,25
10^5	292,51
10^6	2925,12

C. Pseudonym Assignment Protocol

The proposed pseudonym assignment protocol of PRIPAY is performed when an MS wants to have anonymous access to a remote MorSP (see Figure 3). In this paper, we analyze the protocol execution over 3G, omitting the rest technologies (2G, WLAN, WiMAX and 3G-WLAN) that are deployed in a similar way. The protocol functionality and execution are independent of the specific features of the underlying mobile/wireless technology, facilitating maximum transparency and portability. For the analyzed 3G scenario, the network entities that participate are: i) MS, ii) SGSN, iii) PSP, iv) HLR/HSS, v) GGSN and vi) MorSP. Prior to the protocol execution, it assumed that MS has been authenticated and attached to the network. Moreover, we assume that there is a pre-established secure channel between the MorSP and the 3G network based on a Service Layer

 ISBN: 978-1-61208-231-8

Agreement (SLA). The proposed protocol is called before the Packet Data Protocol (PDP) activation procedure, which creates a context that contains all the service parameters of a connection to an external network by means of end-point addresses, quality of service, etc.

The pseudonym assignment protocol execution is triggered (step 1) by a Privacy Service Context Request message that MS sends to SGSN, indicating the mobile subscriber's wish for traceable anonymous access to a remote MorSP (e.g., ssl.ds.unipi.gr). Upon receiving this message, SGSN retrieves the permanent identity of MS (i.e., IMSI) and sends it (i.e., Privacy Service Request message) together with the MorSP address to PSP (step 2). The latter generates a new pseudonym for the specific subscriber, as described in section II.B, and, then, sends it together with the subscriber's IMSI and the remote MorSP address to HLR/HSS for updating the operator database (Privacy Update Request message) (step 3). HLR/HSS confirms updating by replying with a Privacy Update Confirm message. After that (step 4), PSP obtains the digital certificate of the remote MorSP, which is required for providing authentication and integrity between the mobile operator and MorSP as well as encrypting specific fields in the communication between MS and MorSP, as presented below.

At step 5, PSP initializes a digital signature and encryption process as follows: Let M denote the generated pseudonym of MS. PSP computes a message digest h(M) of the pseudonym, using a hash function (e.g., SHA1), and, then, produces a digital signature of the pseudonym $DS=E[KP_{PSP}, h(M)]$, using the computed h(M) as well as the private key of PSP (i.e., KP_{PSP}), (i.e., PSP represents the mobile operator). The produced digital signature, which authenticates the issuing mobile operator and provides integrity to the generated pseudonym, is concatenated with M, creating a new value N (i.e., N= DS||M). PSP encrypts N using MorSP's public key (i.e., KU_{MorSP}), obtained from the digital certificate of MorSP, as $C=E[KU_{MorSP}, N]$ ensuring its confidentiality. Next, PSP sends to GGSN a Privacy Context Request that includes C and the MorSP address to GGSN. The latter sends to PSP a Privacy Context Confirm message indicating the successful reception of C and MorSP address. At step 6, PSP sends a Privacy Service Response message to SGSN that includes the MorSP's address. The latter forwards the MorSP address to MS in a Privacy Service Context Response message.

In step 7, a primary PDP context is activated, which creates internal service tunnels within the mobile network for the data flow and assigns an external IP address (i.e., static or dynamic) to MS. In the same step (i.e., step 7), GGSN sends C to MorSP through a pre-established secure channel (e.g., a VPN). Next, MorSP decrypts C using its private key (i.e., KP_{MorSP}) to obtain N, and, then, verifies the digital signature DS (N= DS||M), using the PSP public key (i.e., KU_{PSP}). If the digital signature DS is not valid, MorSP rejects the provided pseudonym. Otherwise, (i.e., in case of a successful verification of DS), MS may have anonymous access to MorSP using the pseudonym M. It is important to mention that if MS wants to have access to another MorSP, a new pseudonym will be requested and a new primary PDP context will be activated in which a new IP address will be allocated to MS.

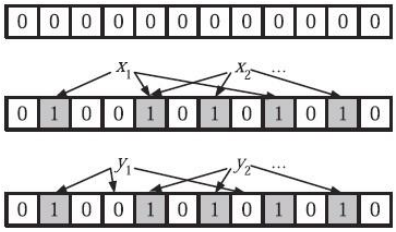


Figure 2. An example of a bloom filter taken from [8]. The filter begins as an array of all 0s. Each item in the set x_i is hashed k=3 times, with each hash yielding a bit location; these bits are set to 1. The element y_1 is not in the set, since a 0 is found at one of the bits. The element y_2 is either in the set or the filter has yielded a false positive.

III. EVALUATION

In this section, we attempt to evaluate the proposed privacy architecture by analyzing its advantages and possible drawbacks. The main objective of PRIPAY is to ensure privacy to mobile users, while enabling anonymous micropayments through the mediation of mobile/wireless operators. The identity or any other personal information of users, such as credit card details etc., is never disclosed to anyone, whilst MorSPs receive only verifiable pseudonyms. Every time a user accesses a remote MorSP, it is assigned to it a different pseudonym, guaranteeing unlinkability. Therefore, the accessed MorSP cannot link preferences and behaviors of the user or track its location. To avoid using the same pseudonym for a second time in a particular CTP, PRIPAY utilizes a bloom filter that allows PSP to efficiently verify that a new generated pseudonym has not been previously assigned. The time needed for this operation is a fixed constant O(k), independent of the number of elements (i.e., assigned pseudonyms) already in the set. Although pseudonym verification may present false positives, their probability p can be relatively low with no functional implication to PRIPAY and negligible impact on its performance (i.e., PSP has to repeat the procedure of generating a new pseudonym and verifying its freshness using the bloom filter).

The proposed architecture allows MS to use one Radio Resource Control (RRC) connection and activate multiple primary PDP contexts that each of them employs a different IP address. In this way, MS may access several MorSPs (using the same RRC), not only with a different pseudonym, but also with a different IP address. If MS uses the same IP address to access different MorSPs, they may collaborate each other compromising unlikablity. An alternative solution would be MS to drop the RRC connection and establish a new one in order to obtain a new IP address, but this may deteriorate the overall network performance and the usability of PRIPAY.

PRIPAY incorporates a set of security features (e.g., digital certificates, public key cryptography, digital signature, etc.) in order to protect its operation and prevent the occurrence of malicious actions. Towards this direction, the generated pseudonyms are digitally signed using the issuer's (i.e., mobile operator) private key and encrypted

 ISBN: 978-1-61208-231-8

using the remote MorSP public key. In this way, we achieve non-repudiation and security against misbehaving MorSP. Moreover, since there is a pre-established secure channel between the mobile operator and the MorSP, the conveyance of C over the public Internet does not pose any security risk, such as replay attacks, man-in-the-middle attacks or modification in the exchanges messages. The generated pseudonyms of a mobile operator, which have been assigned to its subscribers for accessing remote MorSPs during a CTP, are stored in the HLR/HSS database. HRL/HSS already stores sensitive users' (i.e., identities, locations, billing data, etc.) and network information (i.e., authentication information) and, thus, all the security measures and procedures required to protect it and the included information are in place. Hence, no extra security measure is required to protect the generated pseudonyms from internal or external attacks. Moreover, any information exchange between the mobile operator and remote cooperative MorSPs that refer to pseudonyms or charging will be carried encrypted out using public key cryptography.

From the viewpoint of m-commerce, the proposed architecture constitutes an efficient solution for micropayments, since it delegates the billing process to mobile operators. Each operator has already established a micropayment platform to charge mobile subscribers for the network usage, as charges mainly refer to an amount of short duration phone calls, short messages service (SMS) and small volume data sessions. Thus, a mobile operator that installs PRIPAY, may aggregate and charge carried micropayments together with the bills of mobile phones, every CTP. The mobile operator is also able to verify and trace all the used pseudonyms (i.e., traceability) charged by cooperative MorSP within a specific CTP, because the HLR/HSS database is extended to store the assigned pseudonyms for each registered IMSI as well as the remote MorSPs that have been issued for.

The delegation of charging to mobile operators enable micropayments and, in general, financial transactions of mobile subscribers with remote MorSP, without the need of credit cards or specialized accounts (e.g., paypal). This is especially useful for users that do not like credit cards (or specialized accounts) or they don't want to use them either for security reasons or privacy considerations. Moreover, using PRIPAY, the mobile users do not have to complete time-consuming and error prone forms on the reduced-sized screens of MSs.

The deployment of the proposed architecture does not impose extensive modifications to the current technology and existing infrastructure of mobile/wireless operators. It requires: a) the introduction of PSP within the core network of the operator which generates and assigns pseudonyms; b) the development of four new MAP-based messages that are exchanged between SGSN, PSP and HLR/HSS; c) the extension of the HLR/HSS database scheme in order to include the assigned pseudonyms for each IMSI as well as the remote MorSP for which each pseudonym has been issued for; and d) the development of a lightweight application that resides at MS and enables the user to initiate PRIPAY as well as the related communication messages with SGSN. Therefore, the PRIPAY installation and operation do not requires much investment from the operators. On the other hand, PRIPAY will increase the operators' income by increasing the network usage and the related traffic as well as returning a small share of the PRIPAY turnover to them.

Finally, a possible drawback of PRIPAY has to do with the fact that the activation of multiple primary PDP contexts leads to the allocation of multiple IP addresses. This may cause an administrative problem to the operator, as it may exhaust the available IP addresses at GGSN. However, it has to be mentioned that this is enabled only when an MS wants to have anonymous access to several MorSP, simultaneously, using the same RRC connection, which is not the normal case.

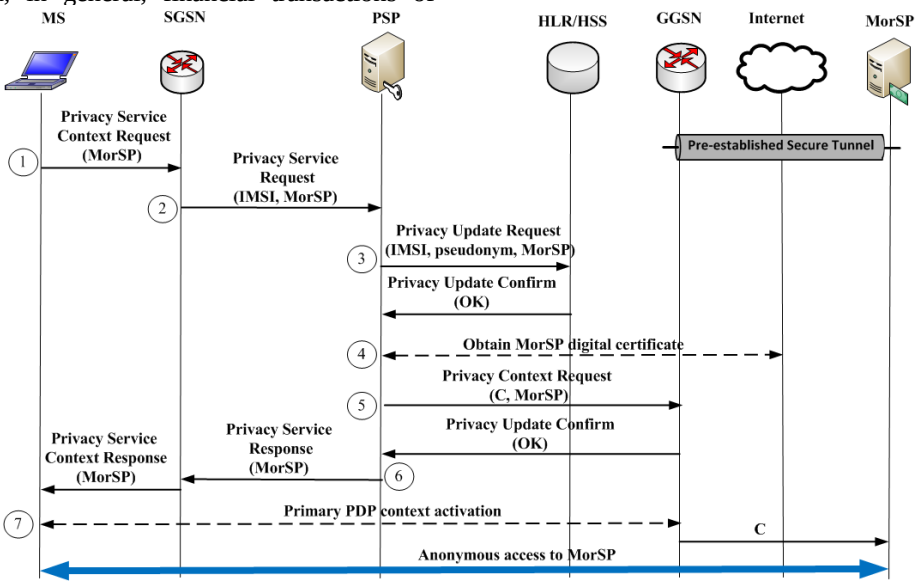


Figure 3. Pseudonym assignment protocol

IV. RELATED WORK

There is a rather limited literature that deals with privacy in mobile/wireless networks. Bessler et al. [9] have proposed a privacy preserving architecture that ensures presence and location privacy in the context of web services, specified by the Parlay X standard. In this architecture, a server, called Privacy Service (resides within the mobile/wireless network), generates pseudonyms for the registered MSs. In order to achieve authentication and authorization, keyed hash chain values are employed between MSs and the Privacy Service. Although this architecture offers an adequate level of privacy, its main drawback is that the involved MSs should execute cryptographic algorithms increasing energy consumption. To address this limitation, Ajam [10] has proposed to incorporate within the deployed Parlay X gateway a privacy web service, which is responsible for managing and ensuring the privacy of MSs. This privacy web service uses a pseudonym database to map pseudonyms to real identities or subscribers' numbers. The main limitation of this architecture is that it provides privacy only for services that are based on OSA/Parlay.

Gritzalis et al. [11] proposed a mechanism called Pythia that ensures privacy in e-commerce and offers both traceability and anonymity. The main idea of this mechanism is that the sender of a message can be authenticated at the receiver, without the latter knowing the former's identity. However, the sender reveals its identity in an intermediary, in order to ensure traceability. This mechanism uses a cryptographic token, which is distributed to the involved users through a TTP. As the employed token is not protected for confidentiality and data integrity, the employment of an additional general purpose security mechanism like the SSL protocol is required increasing the overall operation cost.

Finally, there are some third-party commercial micropayment systems that leverage micropayment transactions through mobile operators [12], [13]. Initially, service and cooperation agreements are required between the micropayment providers and i) the mobile/wireless network operators that will allow their subscriber to use the provided payment systems; and ii) MorSPs that accept payments through the deployed third-party micropayment systems. During a transaction, a mobile subscriber sends its mobile phone number to a MorSP, and the latter sends back to the subscriber's mobile phone an SMS including a random number. The subscriber must submit this number back to MorSP to prove that it is the legitimate owner of the mobile phone number. In this way, all payments made by the mobile subscriber are charged to its mobile phone bill by its operator. Although such systems enable micropayments, they do not offer privacy services, fact that MorSPs may take advantage for their own purposes. For example, MorSPs may use the collected phone numbers for advertisement purposes.

V. CONCLUSIONS AND FUTURE WORK

PRIPAY leverages the trust relationship between mobile users and mobile operators offering anonymous and secure micropayments. Each time a user accesses a remote MorSP, it is assigned a different pseudonym, guaranteeing anonymity and unlinkability. Thus, the accessed MorSP cannot link preferences/behaviors of the user or track its location. The generated pseudonyms are signed using the mobile operator's private key and encrypted using the remote MorSP public key. Thus, their conveyance over the Internet does not pose any security risk. PRIPAY eliminates the need of credit cards or specialized accounts (e.g., paypal), a feature especially useful for users that do not want to use credit cards or specialized accounts for security or privacy considerations. The charging process of micropayments can be easily performed, since the mobile operator can aggregate and charge carried micropayments along with the bills of mobile phones in every CTP. The deployment of the proposed architecture does not impose extensive modifications in the existing infrastructure of mobile/wireless operators. As a future work, we plan to perform simulations to estimate and evaluate the performance (i.e., overhead, possible delays and the energy consumption at the level of mobile devices) of the pseudonym assignment protocol of PRIPAY.

REFERENCES

[1] S. Teltscher and S. Parkes, ITU, http://www.itu.int/newsroom/press_releases/2010/06.html [retrieved: September 2012]

[2] I. A. Getting, "The Global Positioning System," IEEE Spectrum, Vol. 30, pp. 36-47, December 1993.

[3] U. Varshney, R. J. Vetter, and R. Kalakota, "Mobile e-commerce: a new frontier", IEEE Computer, Vol. 33, No. 10, pp. 32-38, October 2000.

[4] European Parliament, Directive 2006/24/EC of the European Parliament and of the Council, March 2006.

[5] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management – v0.34", Aug. 2010.

[6] M. V. Tripunitara and T. S. Messerges, "Resolving the micropayment problem", IEEE Computer magazine, Vol. 40, No. 2, pp. 104-106, 2007.

[7] A. Broder and M. Mitzenmacher, "Network applications of bloom filters: a survey", Internet Mathematics, Vol. 1, No. 4, pp. 485-509, July 2003.

[8] 3GPP TS 23.234 (v11.0.0), "3GPP system to WLAN interworking; system description", Release 11, Sept. 2012.

[9] S. Bessler and O. Jorns, "A privacy enhanced service architecture for mobile users", in Proceedings of the third IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom 2005), pp. 125 - 129, Hawaii, USA, March 2005.

[10] N. Ajam, "Privacy based access to Parlay X location services", in Proceedings of the Fourth International Conference on Networking and Services (ICNS 2008), pp. 204-206, Guadeloupe, France, March 2008.

[11] D. Gritzalis, K. Moulinos, J. Iliadis, C. Lambrinoudakis, and S. Xarhoulakos, "Pythia: towards anonymity in authentication", in proceedings of the IFIP 16th International Conference on Information Security (SEC 2001), pp. 1-17, Paris, France, June 2001.

[12] Mcoin mobile payments, http://www.mcoin.com [retrieved: September 2012]

[13] Zong a paypal service, http://www.zong.com [retrieved: September 2012]

 ISBN: 978-1-61208-231-8

Ambient Intelligence for Outdoor Activities Support

Possibilities for Large-Scale Wireless Sensor Networks Applications

Peter Mikulecky, Petr Tucnik
Faculty of Informatics and Management
University of Hradec Kralove
Hradec Kralove, Czech Republic
peter.mikulecky@uhk.cz; petr.tucnik@uhk.cz

***Abstract*— This paper is devoted to a recently running project with a purpose of getting some useful feedback from the interested community. The main point of the project is an attempt to apply approaches developed in the scope of the Ambient Intelligence area and usually implemented indoor (eg., intelligent homes) also in various fields suitable for large-scale outdoor activities (esp. working) applications, like water resources management, forestry, etc. The paper is oriented on investigation and sketching of some possibilities of large scale intelligent sensor network solutions for multi-agent based application in various areas where outdoor activities are frequent, but also where people working outdoor might need some more support because of possible hazardous situations that could appear. All the presented ideas are based on our recent project *SMEW: Smart Environments at Workplaces* that is oriented on bringing more intelligence to workplaces in general, but it has been oriented prevailingly on indoor working activities. Extending the approaches already developed in its scope to selected outdoor activities seems to be very challenging and useful.**

Keywords-wireless sensor networks; large-scale applications; ambient intelligence; outdoor activities

I. INTRODUCTION

When speaking about outdoor activities from the point of view of possible Ambient Intelligence (AmI) applications intended to provide certain support to the people working or simply situated in an outdoor environment, it is impossible to omit recent achievements in the area of large-scale wireless sensor networks. Related to the Ambient Intelligence research, we have to mention the notion of Large-scale Ambient Intelligence [1].

The notion Large-scale Ambient Intelligence was firstly used in [1]. Here, true large-scale AmI realization meant that the users were able to acquire whatever, whenever and wherever. In this concept it is understood, that the AmI vision would be extended from anytime-anywhere to anytime-anywhere-anything. In addition to incorporating intelligence in sensor nodes within a sensor network, Iqbal et al. [1] proposed to upgrade this vision to the next level where these geographically distributed intelligent sensor networks would become intelligent sensor resources accessible to the users anytime-anywhere.

In our earlier papers [2][3][4], we started with some contemplations related towards possibilities of using ambient intelligence approaches in an outdoor environment, especially for river basin management. Here some approaches based on knowledge-based system applications for a particular river basin control were described. The purpose of the knowledge-based system deployed was in supporting decision making processes of the river basin managers. Nevertheless, the approaches used were a bit narrowly focused, intending to support just decision making of several persons responsible for the river basin control. Other people in the vicinity of the river have not been involved. In the case of, e.g., flooding threats the only informed people were the river basin managers, but not the other people potentially endangered by the threading situation. Therefore we started to think about the possibility of enhancing in this particular case the river basin area by a wireless sensor network with some new functionality, involving also the people working or located in the area, potentially endangered by flash floods, forest fire, or other possible environmental catastrophes. In this paper, we intend to go further with the ideas how ambient intelligence used in "large-scale" over a wireless sensor network throughout the open natural environment could be beneficial in supporting various important activities, performed outdoor, in nature. We present here some ideas about possibilities for outdoor large-scale ambient intelligence focused also on such areas, where environmental catastrophes with disastrous effects could appear.

The structure of the paper is as follows:

After the introduction, the second part is devoted to related work in the area. Here, we mention several interesting papers trying to deploy wireless sensor networks for environmental applications. However, these applications lack the ambient intelligence functionality so far, they are just oriented on data collection and processing from a large environmental area. The collected data are broadcasted to a central point, where they are used as support for decision making of certain persons with various responsibilities related to the area monitored. At the end of the second part, we explain importance of ambient intelligence applications for certain types of outdoor activities and we describe a scenario how ambient intelligence applications over a large-scale wireless sensor networks can be beneficial there.

 ISBN: 978-1-61208-231-8

The third part of the paper sketched briefly some ideas for functionality of large-scale ambient intelligence applications for outdoor activities support. Fourth part of the paper is a summary of presented ideas with a view towards further research.

II. RELATED WORK

Outdoor-oriented applications of Ambient Intelligence approaches should be undoubtedly based on recent achievements in the area of wireless sensor networks. Let us describe shortly a few representative related works in this area, in the second part of this chapter we shall bring an overview of true large-scale outdoor (or environmental) applications based on sophisticated wireless sensor networks.

A. Wireless Sensor Networks

Tremendous effort has been devoted recently to the area of sensor networks and their important applications, as mentioned in [5]. A wireless sensor network is usually a combination of low-cost, low-power, multifunctional miniature sensor devices consisting of sensing, data processing, and communicating components, networked through wireless links [5]. In a typical application, a large number of such sensor nodes are deployed over an area with wireless communication capabilities between neighboring nodes.

There is a number of works dealing with technical possibilities of sensor networks. The book [5] lists a number of results, oriented on context-awareness of sensors and sensor networks. The idea behind context-awareness is, that if sensors could know more about their own context, then they could adapt their behavior and function only when needed and to the extent adequate to the current circumstances. This aspect can be important also for power consumption by the sensor. A lot of work has been done by [6][7][8], interesting survey [9][10]. These works are mainly surveys of recent results in the wireless sensors area and their applications in wireless sensor networks. An excellent survey of environmentally-oriented wireless sensor networks has been written by Corke and his colleagues [11]. They review recent experiments with wireless sensor networks for environmental and agricultural applications; they also provide an interesting critical review of recent research and considers future challenges and opportunitiesin the area of environmental monitoring. A comprehensive, yet bit older, survey of wireless sensor networks applications was written by Arampatzis, Lygeros, and Manesis [12]. They try to survey the numerous applications that utilize wireless sensors, or wireless sensors networks and classify them in five appropriate categories, such as military applications, or environmental monitoring.

B. Large-Scale Environmental Applications

Among a number of recent interesting large-scale environmental applications, we can mention the FieldServer Project [13], and the Live E! Project [14].

The FieldServer Project is oriented on development and networked applications of so-called Field Servers. A Field Server [13] is a wireless sensor network that will enhance the monitoring of environmental factors by allowing sensing nodes to be located at precise locations in fields, reducing overhead installation costs, and allowing for real-time data collection. In Japan, Field Servers were developed for applications at farms. They produce real-time images for security guards, and environmental data for farming. Scientists such as agronomists, physiologists and ecologists can exploit high-resolution real-time images in order to react on any specific situation that deserves or requires some intervention in the environment. Many types of Field Servers have been developed up to now.

The Live E! Project [14] is an open research consortium focused on sharing the digital information related to the living environment. Using the low cost weather sensor nodes with Internet connectivity, a nationwide sensor network was deployed [14]. The network has accommodated more than 100 stations. The application of this weather station network is intended for disaster protection/reduction/recovery and also as educational material for students.

According to Yang [15], watershed management administers water resources within a watershed for different water users. The ultimate purpose of watershed management plan is to maximize the profits of different users meanwhile reducing the possible conflicts that might occur between them. Watershed management can be very efficiently modelled using multi-agent systems, nevertheless, there is just a few works taking into account also catastrophic situations [16].

Some attempts to apply the Ambient Intelligence approaches to disaster management in general are presented in [17], where an architecture is proposed aiming to help in decision-making processes in disaster management. Here, several different environments are considered, namely a smart house, an airport and a paramedics unit assessing a victim of a nuclear disaster.

One of the most significant drivers for wireless sensor network research is without any doubt environmental monitoring. Its potential will not only enable scientists to measure properties that have not previously been observable, but also by ubiquitously monitoring the environment and supplying the related data to relevant supervising bodies they can create a basis of early warning systems for various environmental disastrous situations and their management. As Ruiz-Garcia et al. [18] point out, the relatively low cost of the wireless sensor networks devices allow the installation of a dense population of nodes that can adequately represent the variability present in the environment. They can provide various risk assessment information, for example alerting farmers to the onset of frost damage. Wireless sensor networks based fire surveillance systems were designed and implemented, as well. They can measure temperature and humidity, and detect smoke followed by early warning information broadcasting [19]. Sensors are able to consider certain dynamic and static variables such as humidity, the type of fuel, slope of the land, the direction and the speed of the wind, smoke, etc. They also allow determining the direction and possible evolution of the flame front.

However, apart from other similarly serious environmental disasters, floods are responsible for the loss of

 ISBN: 978-1-61208-231-8

precious lives and destruction of large amounts of property every year, especially in the poor and developing countries. A lot of effort has been put in developing systems which help to minimize the damage through early disaster predictions [20]. On the other hand, as drought periods, opposite to floods, cause lot of damage every year as well [21], also this problem deserves high effort. Interesting solutions to the problems can be found in [22][23] [24].

Cardell-Oliver and her colleagues [6] proposed a novel reactive soil moisture sensor network that reacts to rain storms in such a way, that frequent soil moisture readings were collected during rain (approx. every 10 minutes), but less frequent readings (once a day) were collected when it is not raining. The network includes a node with a tipping bucket rain gauge sensor and, in another part of the landscape, a group of nodes with soil moisture sensors. The node monitoring rain is separated from the nodes monitoring soil moisture, and yet these nodes need to share information, whilst minimizing the time spent sending, receiving and listening to messages.

C. Outdoor Activities Support

In order to support a person's activities outdoor, the geographic location must be identified as important contextual information that can be used in a variety of scenarios like disaster relief, directional assistance, context-based advertisements, or early warning the particular person in some potentially dangerous situations. GPS provides accurate localization outdoors, although is not very useful inside buildings. Outdoor to indoor and vice versa activities localization was investigated, e.g. in [25], by a coarse indoor localization approach exploiting the ubiquity of smart phones with embedded sensors.

Outdoor acting person's support should provide relevant and reliable information to users often engaged in other activities and not aware of some hazardous situations that he or she could possibly encounter. There are only a small number of attempts to solve the related dangerous situations that can be described using the following scenario:

A user appears in a natural environment performing her/his working mission, a kind of leisure time activity (hiking tour, mountaineering, cycling, etc.), or because of being an inhabitant of the area. A sudden catastrophic situation (storm, flash flood, debris flow, etc. could put the person in a risky, if not a life endangering situation. A federated wireless sensor network is ubiquitously monitoring the area and estimating the possible appearance of a dangerous situation. If necessary, the network will proactively broadcast an early warning message to the user, offering her/him related navigation services supporting escape from the dangerous situation.

In the literature, there is only a handful of articles oriented towards a kind of a service to the potentially endangered persons in a natural environment; however, the helpful information to the potentially endangered person is never such complex as we intend to provide in our approach.

For instance, there are some attempts of preventing children from potentially dangerous situations in an urban environment. Probably the first ubiquitous system to assist the outdoor safety care of the schools kids in the real world is described in [26]. The research described there was focused on designing a ubiquitous kid's safety care system capable of dynamically detecting possible dangerous situations in school routes and promptly give advice to kids and/or their parents in order to avoid or prevent some possible dangers. To detect the dangerous situations, it is essential to get enough contexts of real environments in kids' surroundings. This is based on two basic assumptions: (1) a big number of sensors, RFID tags (Radio Frequency Identification tags), and other information acquisition devices are pervasively distributed somewhere in and near school routes, and (2) a kid should carry or wear some devices that can get surrounding context data from the above pervasive devices.

A number of papers are devoted to various solutions for tourist assistance, mainly oriented on context-aware tourist navigation on their routes. The usual approach [27][28] is in deployment of intelligent agents, which collectively determine the user context followed by retrieving and assembling simple information that are wirelessly transmitted and displayed on a Personal Digital Assistant (PDA). However, these tourism oriented applications are usually deployed for navigational purposes, without having capabilities of warning the user from potentially dangerous situations that can appear during their routes.

III. RESEARCH TO BE PERFORMED

The environmentally-oriented wireless sensor networks [29] are mature enough to become a basis for more complex support of various outdoor activities. As Efstratiou [30] pointed out, wireless sensor networks are more and more seen as a solution to large-scale tracking and monitoring applications, but, these networks are usually designed to serve a single application and collected information is commonly available to one authority, usually to the owner of the sensor network.

The usual situation in wireless sensor networks applications is that these networks are just collecting - although usually on a very advanced sophisticated level - data from the environment, with further broadcasting them into some central office for decision support of certain specialists responsible for the area monitored by the sensor network. We believe that we can and must want more from them. For instance, if an intelligent system is deployed over the sensor network with the purpose not only to broadcast the collected data somewhere, but also to provide some processing of the data, evaluation of certain patterns in them significant for certain typical or even unexpected situations in the monitored environment, the whole system would be able to provide at least some early warning messages for people located in the monitored area in order to prevent them from potential endangerments.

According to Efstratiou [30], *the vision for the future generation of sensor networks is of a world where sensing infrastructure is a shared resource that can be dynamically re-purposed and re-programmed in order to support multiple applications. Furthermore, multiple sensor networks (possibly owned by different authorities) can be combined in*

 ISBN: 978-1-61208-231-8

a federated fashion in order to create a more complete picture of the world.

We certainly share this opinion and propose a research, oriented not only on certain combination of sensor networks, as Efstratiou proposes, but also on a design and deployment of an ambient intelligence system over a large-scale environmental wireless sensor network in a potentially risky natural environment that will perform the following tasks:

- Monitoring the usual hydro-meteorological parameters of the environment (air pressure, temperature, humidity, soil moisture, etc.),
- Monitoring indications of possible dangerous situations (seismoacoustic signals, smoke, water on unusual places, etc.),
- Monitoring appearance and movement of animals and human beings in the area,
- Evaluating the data collected from the sensor network and identifying possibly dangerous situations,
- Identification of possibly endangered human beings in the area under monitoring,
- Attempting to contact the persons in danger possibly via their mobile devices and starting to provide all the necessary information and knowledge support aiming to help them escape from the dangerous situation (including eventual alarming of a rescue squad.)

As an example of a system that is in a sense a good candidate to be enhanced according to our just mentioned ideas, we could refer to [31]. The deployed sensor network aimed to assist the geophysics community preventing them from possible dangerous situations. In contrast with at that time existing volcanic data-acquisition equipment the used nodes of the sensor network were smaller, lighter, and consumed less power. The resulting spatial distribution greatly facilitated scientific studies of wave propagation phenomena and volcanic source mechanisms. Certainly, we can imagine a number of potentially dangerous situations that can endanger people working closely to the volcano. Enhancing the purely geophysical sensor networks by the features mentioned above could improve the safety of working near the volcano.

Another example belongs also to the area of potentially dangerous workplaces. The result of [32] seems to be one of those attempts that aimed directly at developing a sensor networks for monitoring possible dangerous situations in a large yet closed environment - a coal mine. Nevertheless, the experience with early warning sensor network in a Chinese coal mine is very good and inspirational [32].

IV. CONCLUSION AND FUTURE WORK

Our recent project *SMEW: Smart Environments at Workplaces* is oriented on bringing more intelligence to workplaces in general, but it has been oriented prevailingly on indoor working activities. Extending the approaches already developed in its scope to selected outdoor activities seems to be very challenging and useful.

Implementation of the ideas sketched in the paper still needs a lot of future work. We are working recently on a multi-agent architecture capable to process data provided by the underlying wireless sensor network in such a way that a model of the monitored environment will be created as a basis for further steps of the whole systems. Based on the created model, the multi-agent architecture should by capable to identify any deviation from the expected state of the environment, decide about possible action to be launched, and communicate with any person appearing in the potentially dangerous situation throughout the environment. Of course, at least the following research tasks must be solved:

- Design of the multi-agent architecture over the wireless sensor network implemented throughout the outdoor environment;
- Employment of a suitable decision-making mechanism that will serve in selecting the most appropriate actions to be possibly launched;
- Decide about the most appropriate way of communication with potentially endangered persons appearing in the monitored environment;
- Implement the multi-agent architecture over a real and carefully chosen large-scale wireless sensor network in a real outdoor environment (a forest, a watershed, or any other suitable environment) and evaluate it.

Ambient intelligence approaches have recently proven their usefulness when implemented indoor (intelligent homes or households). We are convinced that outdoor implementations have a large applicability as well and can be at least equally useful.

ACKNOWLEDGMENT

This work was supported by the Czech Science Foundation project GACR P403/10/1310 „*SMEW – Smart Environments at Workplaces*“.

REFERENCES

[1] M. Iqbal, H. B. Lim, W. Wang, and Y. Yao, “A sensor grid infrastructure for large-scale ambient intelligence”, in 2008 Ninth International Conference on Parallel and Distributed Computing, Applications and Technologies, pp. 468-473, IEEE, 2008.

[2] P. Mikulecky, K. Olsevicova, and D. Ponce, “Knowledge-based approaches for river basin management”, Hydrol. Earth Syst. Sci. Discuss., 4, pp. 1999–2033, 2007.

[3] P. Mikulecký, D. Ponce, and M. Toman, “A knowledge-based decision support system for river basin management”, in River Basin Management II, C.A.Brebbia, Ed., Southampton: WIT Press, 2003, pp. 177-185.

[4] P. Mikulecký, D. Ponce, and M. Toman, “A knowledge-based solution for river water resources management”, in Water Resources Management II, C.A. Brebbia, Ed., Southampton: WIT Press, 2003, pp. 451-458.

[5] S. Loke, Context-Aware Pervasive Systems, Boca Raton: Auerbach Publications, 2007.

[6] R. Cardell-Oliver, K. Smettem, M. Kranz, and K. Mayer, “A reactive soil moisture sensor network: Design and field evaluation”, Int. Journal of Distributed Sensor Networks 1, pp. 149-162, 2005.

 ISBN: 978-1-61208-231-8

[7] E. Elnahrawy and B. Nath, "Context-aware sensors", in Proc. 1st European Workshop on Wireless Sensor Networks, pp. 77-93, 2004.

[8] Q. Huaifeng and Z. Xingshe, "Context-aware Sensornet", in Proc. 3rd International Workshop on Middleware for Pervasive and Ad-Hoc Computing, Grenoble, ACM Press, pp. 1-7, 2005.

[9] I. F. Akyldiz, W. Su, Z. Sankarasubramaniam, and E. Cayrici, "A survey on sensor networks", IEEE Communications Magazine 40, pp. 102-114, 2002.

[10] D. Puccinelli and Haenggi, M., "Wireless sensor networks: Applications and challenges of ubiquitous sensing", IEEE Circuits and Systems Magazine, pp. 19-29, 3rd Quarter 2005.

[11] P. Corke, T. Wark, R. Jurdak, W. Hu, P. Valencia, and D. Moore, "Environmental wireless sensor networks", Proceedings of the IEEE, Vol. 98, No. 11, pp. 1903-1917, November 2010.

[12] Th. Arampatzis, J. Lygeros, and S. Manesis, A Survey of Applications of Wireless Sensors and Wireless Sensor Networks, in Proc. of the 13th Mediterranean Conference on Control and Automation, Limassol, Cyprus, pp. 719-724, June 2005.

[13] S. Ninomiya, T. Kiura, A. Yamakawa, T. Fukatsu, K. Tanaka, H. Meng, M. Hirafuji, Seamless Integration of Sensor Network and Legacy Weather Databases by MetBroker, In 2007 International Symposium on Applications and the Internet Workshops (SAINTW'07), IEEE, p. 68, 2007.

[14] S. Matsuura, et al., LiveE! Project: Establishment of Infrastructure Sharing Environmental Information. In 2007 International Symposium on Applications and the Internet Workshops (SAINTW'07), IEEE, p. 67, 2007.

[15] I.-C. Yang, Modeling Watershed Management with an Ecological Objective - A Multiagent System Based Approach. PhD Dissertation, University of Illinois at Urbana-Champaign, 2010.

[16] L. Brouwers, K. Hansson, H. Verhagen, and M. Boman, Agent Models of Catastrophic Events. In Proceedings of Modelling Autonomous Agents in a Multi-Agent World, 10thEuropean workshop on Multi Agent Systems, Annecy, 2001.

[17] J.C. Augusto, J. Liu, and L. Chen, Using Ambient Intelligence for Disaster Management. In Knowledge-Based Intelligent Information and Engineering Systems, Proc. KES 2006, LNCS 4252, Berlin and Heidelberg: Springer, pp. 171-178, 2006.

[18] L. Ruiz-Garcia, L. Lunadei, P. Barreiro, and J.I. Robla, A Review of Wireless Sensor Technologies and Applications in Agriculture and Food Industry: State of the Art and Current Trends. Sensors 9, pp. 4728-4750, 2009.

[19] J. Lloret, M. Garcia, D. Bri, and S. Sendra, A Wireless Sensor Network Deployment for Rural and Forest Fire Detection and Verification. Sensors 9, pp. 8722-8747, 2009.

[20] V. Seal, A. Raha, S. Maity, et al., A Simple Flood Forecasting Scheme Using Wireless Sensor Networks. International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.3, No.1, pp. 45-60, 2012.

[21] H. - Y. Kung, J.-S. Hua, and C.-T. Chen, Drought Forecast Model and Framework Using Wireless Sensor Networks. J. of Inf. Science and Engineering 22, pp. 751-769, 2006.

[22] R. Marin-Perez, J. García-Pintado, and A. Skarmeta Gómez, A real-time measurement system for long-life flood monitoring and warning applications. Sensors 12, pp. 4213-4236, 2012.

[23] Y. Zhang, L. Luo, J. Huo, and W. Zhu, An Eco-Hydrology Wireless Sensor Demonstration Network in High-Altitude and Alpine Environment in the Heihe River Basin of China. Wireless Sensor Network, Vol. 4 No. 5, pp. 138-146, 2012.

[24] E. Basha and D. Rus, Design of Early Warning Flood Detection Systems for Developing Countries, in Proceedings of the Conference on Informations and Communication Technologies and Development, Bangalore, India, 2007.

[25] A. Parnandi, K. Le, P. Vaghela, A. Kolli, K. Dantu, S. Poduri, and G. S. Sukhatme, Coarse In-Building Localization with Smartphones, Proc. of the MobiCASE 2009, pp. 343-354, 2009.

[26] K. Takata, Y. Shina, H. Komuro, M. Tanaka, M. Ide, and J. Ma, Designing a Context-Aware System to Detect Dangerous Situations in School Routes for Kids Outdoor Safety Care, in L.T. Yang et al. (Eds.): EUC 2005, LNCS 3824, pp. 1016-1025, Berlin: Springer, 2005.

[27] G.M.P. O'Hare and M.J. O'Grady, Gulliver's Genie: a multi-agent system for ubiquitous and intelligent content delivery, Computer Communications 26, pp. 1177–1187, 2003.

[28] O. Krejcar, Threading Possibilities of Smart Devices Platforms for Future User Adaptive Systems, in Intelligent Information and Database Systems, Berlin: Springer, pp. 458-467, 2012.

[29] J. K. Hart and K. Martinez, Environmental Sensor Networks: A revolution in the earth system science?, Earth-Science Reviews 78, pp. 177 – 191, 2006.

[30] Ch. Efstratiou, Challenges in Supporting Federation of Sensor Networks, in NSF/FIRE Workshop on Federating Computing Resources, 2010.

[31] G. Werner-Allen, K. Lorincz, M. Welsh, O. Marcillo, J. Johnson, M. Ruiz, and J. Lees, Deploying a wireless sensor network on an active volcano. IEEE Internet Computing, 10(2), pp18-25, 2006.

[32] X. Wang, X. Zhao, Z. Liang, and M. Tan, Deploying a Wireless Sensor Network on the Coal Mines, in Proceedings of the 2007 IEEE International Conference on Networking, Sensing and Control, London, UK, pp. 324-328, April 2007.

 ISBN: 978-1-61208-231-8

Optimized Flow Management using Linear Programming in Integrated Heterogeneous Networks

Umar Toseef *†, Yasir Zaki†, Andreas Timm-Giel* and Carmelita Görg†
*Institute of Communication Networks, Hamburg University of Technology, Hamburg, Germany
Email: {umar.toseef, timm-giel}@tuhh.de
†TZI ComNets, University of Bremen, Bremen, Germany,
Email: {yzaki,cg}@comnets.uni-bremen.de

***Abstract*—There have been tremendous advances over the past decades when it comes to wireless access technologies. Nowadays, several wireless access technologies are available everywhere. Even mobile devices have evolved to support multiple access technologies (e.g., 3G, 4G or WiFi) in providing the best possible access to the Internet. However, all of these devices can communicate using one access technology at a time. There is a need of the integration of all these access technologies to cooperate and work simultaneously in a heterogeneous environment from which both the end users, as well as, the mobile operators can benefit. This paper investigates how to tackle the simultaneous usage of wireless access technologies in the downlink. For this purpose, a practical example of 3GPP LTE and non-3GPP WLAN integrated heterogeneous network is considered. Furthermore, a novel decision mechanism is proposed, that focuses on optimizing the flow management of user traffic flows based on a mathematical formulation of the system. The mathematical model is implemented using the Linear Programming techniques. The paper demonstrates the gains that are achieved from using such innovative decision mechanism, as well as, the benefits that arise from the simultaneous usage of wireless heterogeneous accesses.**

Keywords: ***LTE and WLAN interworking, User QoE optimization, Linear programming, Access link modeling***

I. Introduction

4G communication networks are purely IP-based, and characterized by independent drives, such as: users, network operators, and service providers, etc. Due to the maturity of the current communication paradigms, there is no point in highlighting the importance of heterogeneous wireless technologies and their co-existence in the future wireless access networks. When it comes to heterogeneous wireless technologies, one can discern various prevailing standards in the current communication market, such as 3GPP, non-3GPP, 3GPP2, etc. Both 3GPP and non-3GPP are of core importance, however it is common conception that most of the non-3GPP technologies need less investment and operation & maintenance cost compared to 3GPP technologies. Furthermore, the widespread usage of non-3GPP wireless access technologies, like IEEE 802.11 has shown its practical usefulness in many environments. Now, that the market is ready to accept both 3GPP and non-3GPP technologies, this provisions that end consumers should be enabled to make efficient use of the services extended through both technologies. Even more, the 3GPP standards has already come up with such integration standards [13].

The System Architecture Evolution (SAE) 3GPP specified allows mobile users to roam between 3GPP and non-3GPP access technologies. In order to provide users with seamless mobility, Proxy Mobile IPv6 (network based mobility) and Dual Stack Mobile IPv6 (host based mobility) have been proposed [13]. The 3GPP SAE architecture, however, has certain limitations when it comes to supporting multi-homed users. This implies that a user can be associated with one of the available access networks but cannot connect to more than one network simultaneously.

The focus of this work is to firstly investigate how the multi-homing support can be realized in 3GPP SAE architecture. Secondly, how the network operators can make an optimum use of aggregated bandwidth resources and network diversity in a multi-homing scenario through the flow management. The rest of the paper is organized as follows: related work has been discussed in Section II, Section III describes how the current 3GPP SAE architecture can be extended to provide users with multi-homing support. Section IV describes the importance of flow management function in a heterogeneous network, and Section V explains the linear programming technique to do optimized flow management operation. Finally, Section VI provides the proof of concepts through the discussion of simulation results of an investigated realistic scenario.

II. Related Work

A number of research studies can be found making use of cross-layer techniques and soft handover to optimize handover cost in terms of packet delay and loss in heterogeneous networks. For example, Song and Jamalipour [2] describes an intelligent scheme of vertical handover decisions in selecting the best handover target from the several candidate heterogeneous networks. Several other proposals have been made to improve the performance of cellular and 802.11 networks. Song et. al. [3] has discussed admission control schemes to improve the performance of integrated networks. Fei and Vikram [5] proposes a service differentiated admission control scheme based on semi-Markov chain which is although very accurate but has high computational complexity. Similarly, Zhai et. al. [6] has shown that by controlling the collision probability with the help of input traffic rate of users, the maximum throughput can be achieved by keeping 802.11 network in non-saturated state. Other studies are focused on developing solutions for

 ISBN: 978-1-61208-231-8

load balancing in the integrated heterogenous networks. Such a proposal can be found in [7] where policy based load balancing framework has been presented to effectively utilize the aggregated resources of loosely coupled cellular/WLAN network. In this work, we explore the practical limits of achievable performance in a heterogeneous network scenario by going down to the MAC layer functionalities of involved access technologies. The goal is to maximize the spectral efficiency of network bandwidth resources and fulfill the application QoS requirements at the same time. In contrast to other studies, we provide an analytical solution to the problem which adapts time varying channel conditions of the user and dynamically decides the best network paths for user traffic flows in order to achieve system wide optimized performance and improved user QoE. The focus of this work is, however, restricted to the downlink of access technologies.

III. Network simulation model

This work follows the proposal of 3GPP specifications in the integration of 3GPP access technology (namely, LTE) and trusted non-3GPP access technology (namely, legacy WLAN 802.11g) where host based mobility solutions, i.e., Dual Stack Mobile IPv6 is considered. For this purpose, a simulation network model has been implemented using the OPNET [14] network simulator. This includes the detailed implementation of LTE network entities following the 3GPP specifications. As per 3GPP proposal the home agent (HA) function is located at the Packet Data Network (PDN) gateway. The remote server acts as a correspondent node (CN) from where mobile users access application services like VoIP, video, HTTP and FTP (see Fig. 3). A comprehensive description of this heterogeneous network simulator can be found in [9].

It should be noted that our focus is only on the downlink access for LTE and WLAN. This implies that no uplink transmissions are performed for WLAN during the whole simulation time. Instead uplink traffic (e.g., TCP ACK packets etc.) is transmitted by the user through LTE access link.

IV. Flow Management

In the developed simulation environment, a user can communicate simultaneously through 3GPP access technology, i.e. LTE, as well as non-3GPP access networks, i.e., WLAN. The question still remains how a network operator or a user can make use of the two network paths from two access technologies. The answer is to introduce a flow management function at the home agent. The flow management function makes use of the MIPv6 extensions and allows to control the user data rate on each network path. In general, there are two options of managing traffic flows for a multi-homed user. The first option is to carry one complete application traffic flow over one path of choice, this is known as "traffic flow switching". The second option is to divide the traffic flow into several smaller sub-flows where each sub-flow is carried over one network path. This will be called "traffic flow splitting".

If flow management is performed in properly a considerable improvement in network capacity and user satisfaction can be achieved. That is why the decision engine of the flow management function which controls the user data rate over the network paths is of core importance. In order to attain the goals of optimized network performance, the decision engine needs to know the precise information of the available network resources and the user demands. Once this information is available, the decision engine, with the help of proposed mathematical techniques, can optimally assign network resources to the users fulfilling their demands while making use of all available network paths. Though in this work the decision engine of the flow management function is located at the home agent, this may reside at any point inside the core network according to the network hierarchy demands.

The amount of network resources of a wireless network are determined from the designed parameters like frequency spectrum, transmission technology, antenna gains etc. Therefore each network has a fixed amount of network resources and the network performance itself depends on the fact with what (spectral) efficiency these resources are utilized. In order to achieve higher data rates a network resource scheduler should select those users who can attain high spectral efficiency and therefore need less network resources per unit data rate. In this work we adapt the term "network path cost" for the required network resources per unit data rate. For a user, its network path cost can be accessed through cross layer information from the MAC layer of the corresponding access technologies. In the following subsections, it is shown how the network path cost can be computed for users in WLAN and LTE networks.

A. Network path cost for WLAN

Consider a scenario where a WLAN access network consists of a station associated with an access point. Assume that the station is just receiving a downlink traffic flow from the access point and does not transmit anything in the uplink. In this way, there is no contention for medium access. The transmission of one data frame with RTS/CTS enabled takes T_S seconds including the exchange of control frames such as RTS/CTS, SIFS (Short Interframe Space), DIFS (DCF Interframe Space), and ACK frames, where

$$T_S = T_{backoff} + T_{DIFS} + T_{RTS} + T_{CTS} + T_{data} + 3 \cdot T_{SIFS},$$

$$T_{backoff} = \frac{W_{min} - 1}{2} \cdot T_{slotTime},$$

$$T_{DIFS} = T_{SIFS} + 2 \cdot T_{slotTime}$$

All components of T_S except T_{data} can be found in the 802.11 standards. The value of T_{data} can be computed based on the PHY speed of transmission, i.e., $T_{data} = \frac{\sigma}{\varphi}$, where σ is the data frame size in bits, and φ is the PHY transmission speed in [bit/sec]. Accordingly, the maximum downlink capacity η can be estimated as follows: $\eta = \frac{\sigma}{T_S}$ [bit/sec].

It is clear that 802.11 MAC follows the Time Division Multiple Access (TDMA) like scheme, where users share the wireless access medium for short periods of time. Considering resource allocation time interval of 1, a user needs medium access for a fraction τ of the interval to achieve a unit data rate

 ISBN: 978-1-61208-231-8

of 1 bit/sec. τ is actually the network path cost whose value directly depends on T_S, which is the delay experienced in transmitting one data packet of average size σ [bit] operating with PHY speed φ [bit/sec]. That is, $\tau = \frac{T_S}{\sigma}$

B. Network path cost for LTE

In contrast to 802.11, LTE performs a managed scheduling of available bandwidth resources. The smallest unit of bandwidth resource is referred as a physical resource block (PRB) in the LTE specification. Based on the allocated frequency spectrum size, LTE has a certain number of PRBs. The LTE MAC scheduler residing at the eNodeB schedules these PRBs using a 1ms transmission time interval (TTI). The LTE MAC scheduler has a very complex way to assign resources to the associated users. Without digging into the details of the MAC scheduler operation, we focus on the last stage of resource assignment procedure in a certain TTI. On reaching that stage, the MAC scheduler already builds up a list of users which will be transmitting/receiving data in that TTI. For each user entry in the list, there is a corresponding value of the allocated number of PRBs, as well as the channel dependent Modulation and Coding Scheme (MCS) index. These two values are used to lookup the Transport Block Size (TBS) from a table defined in the 3GPP specifications [10]. This is a two-dimensional table, where each row representing one MCS index lists several values of TBS corresponding to the allocated number of PRBs. The obtained TBS value defines the size of the MAC frame transmitted to the user in that TTI. In this way, the user received throughput at the MAC layer in a certain TTI can be estimated if the TBS value for that user is known.

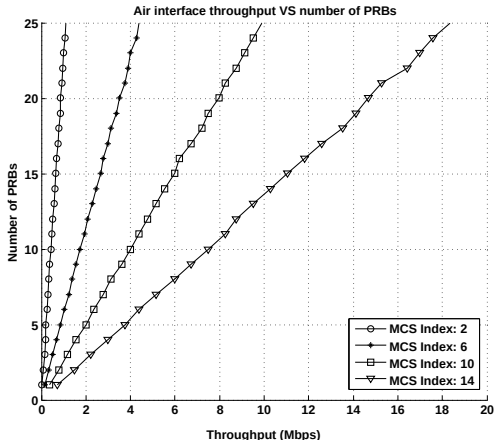


Fig. 1. Relationship of LTE air interface throughput and number of PRBs for different MSC index values [10]. Each curve represents one MCS index.

Fig. 1 shows that for a particular MCS index, the LTE throughput value has almost a linear relationship with the used number of PRBs. If described mathematically, this relationship can be used to determine the required number p of PRBs/TTI to achieve a certain data rate X [kbit/sec] for a user having MCS index i. That is

$$p = C_i \cdot X + K_i$$

C_i is slope of a straight line (as shown in 1) described in units of PRBs/kbps. K_i is the intercept at the y-axis and has units of number of PRBs. It can be noticed that C_i is the data rate dependent part, while K_i is the data rate independent part of network resource requirement for a user with channel conditions mapped to MCS index i.

V. Optimized network resource utilization

When the network path costs for a multi-homed user are known, the problem of optimal resource utilization can be solved using mathematical techniques. In this work, we prefer Integer Linear Programming (ILP) to solve this problem. This choice has been made due to several reasons. In ILP, the optimum solution is guaranteed for a correctly formulated problem, the problem can be extended or restricted by introducing appropriate constraints, it saves some additional implementation work by making use of already available linear programming solvers etc.

Given

U	a set of users
α_j	Data rate dependent part of the LTE link cost in PRBs per kbps for user j, for each $j \in U$
β_j	Data rate independent part of the LTE link cost in PRBs for user j, for each $j \in U$
γ_j	Cost of WLAN link in seconds per kbps for user j, for each $j \in U$
δ_j	Minimum data rate (kbps) demand of a traffic flow destined to user j, for each $j \in U$
Δ_j	Maximum data rate (kbps) allocation for a traffic flow destined to user j, for each $j \in U$
Ω	Number of available PRBs for the LTE access network

Defined variables

X_j	Size of sub-flow in kbps sent over the LTE access link to user j, for each $j \in U$
Y_j	Size of sub-flow in kbps sent over WLAN access link to user j, for each $j \in U$
Z_j	Auxiliary binary variable; its value for a user j is either 1 if $X_j > 0$ or 0 otherwise, for each $j \in U$

Maximize

$$\sum_{j \in U} X_j + Y_j$$

Subject to

1. $\sum_{j \in U} \alpha_j \cdot X_j + \beta_j \cdot Z_j \leq \Omega$
2. $\sum_{j \in U} \gamma_j \cdot Y_j \leq 1$
3. $\delta_j \leq X_j + Y_j \leq \Delta_j$ for each $j \in U$
4. $Z_j \leq X_j \cdot 10^{20}$ for each $j \in U$
5. $Z_j \geq X_j / \Delta_j$ for each $j \in U$
6. $0 \leq X_j \leq \Delta_j$ for each $j \in U$
7. $0 \leq Y_j \leq \Delta_j$ for each $j \in U$
8. $Z_j \in \{0, 1\}$ for each $j \in U$

Fig. 2. Mathematical model for the optimized resource utilization in algebraic form

Fig. 2 shows the formulation of the problem in algebraic form. The model defines U as the set of multi-homed users. Each element of this set has a number of input parameters, e.g. network path costs for LTE (α,β) and WLAN network (γ)

 ISBN: 978-1-61208-231-8

according to the user channel conditions in the corresponding network. The maximum and minimum range of user data rate demands (δ, Δ) which is based on the individual user application. The amount of available network resources in LTE (Ω) and WLAN (which is 1 second) are also considered as input parameters. The output parameters for each user in set U include the assigned data rate over the LTE network and the WLAN network paths (X,Y). It is obvious that the goal of this model is to achieve the highest possible spectral efficiency from the two network access technologies. The higher the spectral efficiency, the higher the network throughput. Hence, the objective is to maximize the user data rate over the two network paths, i.e., X and Y for every multi-homed user.

The model imposes eight constraints which are listed at the bottom of Fig. 2. The first two constraints ensure that the available network resources should not be exceeded when allocating the data rates for users. The third constraint dictates that the user data rate allocation should lie in the specified range. The 4th and 5th constraint determine the value of variable Z based on the X value. If there is a need, a user is allowed to receive its whole demanded data rate over a single network path as shown in constraint number 6 and 7. Constraint 8 is set in order to emphasis that Z is a binary variable which has value either 0 or 1.

It is assumed here that each user is running only one application. For a constant bit rate application, e.g., VoIP or video the minimum data rate is set equal to the maximum data rate in the model input parameters. For TCP based flows, these two values can be set according to the network operator's policy. It should be noted that the problem has been formulated in a way that it guarantees the minimum data rate for all users and then assigns an additional data rate up to the maximum data rate while optimizing the spectral efficiency of the access networks.

In the investigated scenario, the LTE coverage is available in the whole area of user movement while WLAN coverage is limited in a circular area of 100 meter radius around a hotspot. This implies the users always have LTE access available and WLAN coverage is only found in the vicinity of the hotspot (see Fig. 3). During the resource assignment process, the flow management function classifies users into the following three categories (i) users with LTE access only and running VoIP or video applications (ii) users with LTE and WLAN access running any type of application (iii) users running FTP or HTTP applications with LTE access only. Users in the first category must be assigned the required minimum data rate through LTE as there is no other access available for them. Users in the second category are multi-homed users whose data rate will be decided by the aforementioned mathematical model. For users belonging to the third category, they must get their traffic through the LTE path, however, it is not clear how much data rate should be allocated to them in order to achieve the optimized resource allocation objective. This issue is resolved by using the following work around: the users are assigned a WLAN network path cost greater than unity and they are put into the second category. The WLAN network

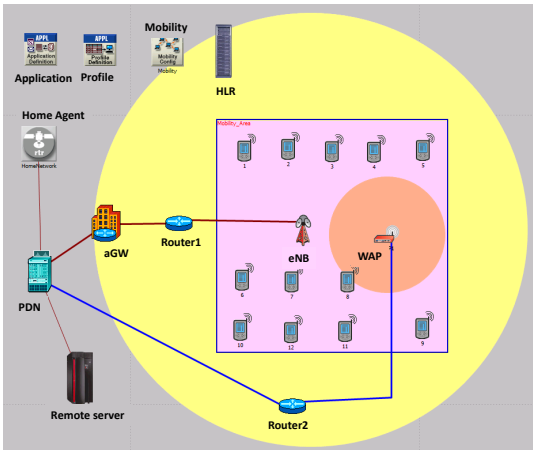


Fig. 3. Overview of the considered simulation scenario in the OPNET simulator. The large circular area shows the LTE network coverage and the smaller circular area shows the WLAN network coverage. The user movement is restricted to the rectangular area inside the large circle.

cost greater than unity will refrain the LP solver to assign any data rate for these users over the WLAN path while the data rate for the LTE path will be decided based on the global objective of the optimized resource allocation.

The resource assignment process by the flow management function is carried out periodically every 100ms in order to adapt to any changes in the user channel conditions. For this purpose user channel condition parameters are obtained through cross layer information from the base stations of the two access technologies. With the help these parameters, costs for each user network path is computed and fed to the above described mathematical model as the input arguments accompanied with the user data rate demands. As described earlier, the mathematical model is formulated using linear programming and solved using the C application programming interface (API) of ILOG CPLEX from IBM [15] which has been integrated inside the OPNET simulator by the authors. The output of this process consists of user data rates on each network path. These decided data rates are then implemented for each user through a traffic shaping function residing at the home agent.

VI. Simulation Results

This section shows the benefits of the proposed approach with the help of simulation results. For this purpose, two scenarios are considered. In one scenario, users do not make simultaneous use of LTE and WLAN access technologies. Instead the user traffic is completely handed over to WLAN as soon as the user enters in the hotspot coverage, otherwise all traffic takes its path through the LTE access. This is the default policy for a multi-homed user according to the 3GPP specifications and therefore it will be referred to as "3GPP HO" case. Whereas, the second scenario extends the 3GPP architecture to supporting the simultaneous use of wireless interfaces, this will be referred to as "Multi-P". In this case user traffic flows are distributed over the WLAN and the LTE

 ISBN: 978-1-61208-231-8

TABLE I
SIMULATION CONFIGURATIONS

Parameter	Configurations
Total Number of PRBs	25 PRBs (5 MHz specturm)
Mobility model	Random Direction (RD) with 6 km/h
Number of users	2 VoIP, 1 HD video & 3 Skype video call, 2 HTPP, 4 FTP downlink users
LTE Channel model	Macroscopic pathloss model , Correlated Slow Fading [1]
LTE MAC Scheduler	TDS: Optimized Service Aware [8], FDS: Iterative RR approach
WLAN technology	802.11g, RTS-CTS enabled, coverage $\approx$ 100 m
VoIP traffic model	G.722.2 wideband codec, 23.05kbps data rate
Skype video model	MPEG-4 codec, 512kbps, 640x480 resolution, 30fps, play-out delay: 250 ms
HD video model	MPEG-4 codec, 1Mbps, 720x480 resolution,
HTTP traffic model	Pag size: constant 100KB, reading time: 12s
FTP traffic model	FTP File size: constant 10 MByte continuous file uploads one after the other.
Simulation run time	10^3 seconds,14 seeds, 98% confidence interval

access network. The traffic flow distribution policy is derived from the output of the optimization problem solved using linear programming. As a result, a user traffic flow is either sent over one network path with the least cost or it is split into two appropriately sized sub-flows each taking one network path to the destination. A reordering buffer at the receiver takes care of sub-flow aggregation and packet reordering in case of flow splitting.

Fig. 3 shows an overview of the simulation model implemented in OPNET. The system is populated with 12 users generating a rich traffic mixture of as shown in Table I. The users move within one LTE eNB cell, and within this cell one wireless access point (or hotspot) is present. It should be noted that in the "Multi-P" scenario the minimum data rate for FTP and HTTP users is assigned as 200kbps while the maximum data rate limit is set to a very high value of 25Mbps.

It's worth mentioning here that in the "3GPP HO" scenario users make vertical handover of hard nature, i.e., the user disconnects completely from one network, and establishes a new connection to the other. Though MIPv6 keeps all IP layer connections alive through seamless handover, users might lose some buffered data on the previously connected network. On the other hand, the "Multi-P" scenario makes users use the WLAN when it is in the coverage, and can still keep the LTE connection and use it simultaneously. As a result, a bandwidth aggregation process of both access links is carried out.

Fig. 4 shows the spider web graph of the average number of successful file downloads per user. A spider web graph is a visualization technique that can show multiple results in one graph, and is used to compare the different scenarios. The graph in Fig. 4 has four different axes, each representing one application. Since all the axes represent the number of file downloads, the algorithm producing the larger shape has the best performance. In this case, it is clear that the "Multi-P" algorithm achieves the best results for all types of user traffic. The reason why TCP based applications accomplish less file downloads is twofold (i) higher TCP throughput helps them download more files as seen in case of FTP (ii) in case of

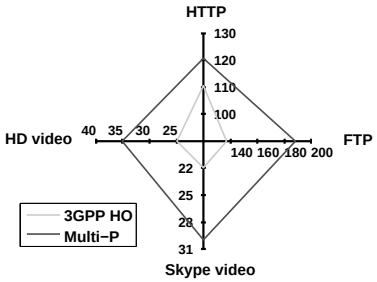
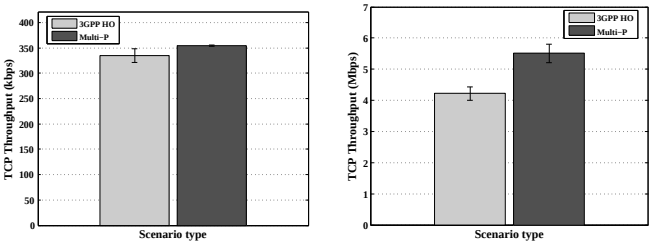


Fig. 4. Overview of downlink service performance. Average number of successfully downloaded files by a user.



(a) Average HTTP user throughput (b) Average FTP user throughput

Fig. 5. TCP download throughput experienced by FTP and HTTP users

"3GPP HO" some TCP connections are aborted during the vertical handover due to excessive packet loss and sudden big changes in TCP round trip time. The second point is explained further in the following.

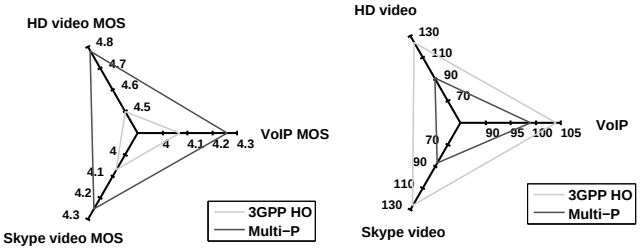
In "3GPP HO" scenario, when the users move from one access network to the other, the data buffered at the base station in the previous network is lost. This is because in the "3GPP HO" case users cannot keep connected to multiple access networks. On the other hand, in the "Multi-P" scenario the loss of buffered data in the network is avoided in the following manner (i) the LTE connection is always kept alive hence no buffered data is lost (ii) in WLAN, the flow management function at the HA sends user traffic on the WLAN link only when the user PHY mode is 9Mbps or higher. This is because when a user enters the 6Mbps mode it implies that the user is almost at the edge of coverage which is a strong indication that loss of the WLAN link is imminent. Hence, no new traffic data is sent over the WLAN link which gives the user a chance to receive the already buffered data at the access point before the loss of the link.

If a large number of packet losses are experienced or excessive packet delays are encountered during the video stream reception, the data download itself does not stop. However such conditions lead to a corrupted video stream reception at the user end which cannot be decoded and therefore its quality cannot be evaluated. In the "3GPP HO" scenario video, users experience packet losses during the handover as explained earlier and, moreover, there is also large end-to-end delay when video data is transmitted through the WLAN network. The reason is as following, when VoIP and video traffic is transmitted over LTE, it is prioritized over FTP to achieve

 ISBN: 978-1-61208-231-8

the required QoS (i.e., throughput and delay). But, in the "3GPP HO" scenario when this traffic type is handed over to WLAN the required QoS cannot always be achieved due to the lack of QoS differentiation support by 802.11g. The "Multi-P" scenario users do not come across such problems because the flow management function can precisely estimate the network capacities and use a network path only if it can support the required data rate. Hence no congestion takes place at the base station and therefore no extreme packet delays are observed. This allows the video users to receive their streaming data without losses and delays and help them achieve higher numbers of successful or decodable video file downloads compared to the "3GPP HO" scenario.

Fig. 5 shows the average TCP throughput as experienced by the FTP and HTTP users in the downlink. The "Multi-P" algorithm achieves approximately 30% more throughput for FTP users by increasing the spectral efficiency of the networks. As for the HTTP performance, it can be seen that the two algorithms show almost similar throughput. This is because the HTTP page size is small enough to be downloaded completely during the TCP slow start phase. In this way, it cannot make full use of the available bandwidth.



(a) Average MOS value (b) Average packet delay (ms)

Fig. 6. VoIP and video service performance

Fig. 6(a) shows the average Mean Opinion Score (MOS) values of VoIP and video services as experienced by the users. MOS gives a numerical indication of the perceived quality of the media received after being transmitted and eventually compressed using codecs. MOS is expressed in one number, from 1 to 5, 1 being the worst and 5 the best. In this work, the MOS values of the wideband VoIP codec and video codec are computed using the modified E-model and Evalvid toolkit as described in [12] and [11], respectively. The "Multi-P" scenario users boast the highest achievable MOS value for individual services. On the other hand, users in the "3GPP HO" scenario suffer from a certain degradation in MOS value. Fig. 6(b) shows the end-to-end packet delay for the three service types. It can be observed that the "Multi-P" scenario once again shows its superiority over "3GPP HO" by providing shorter end-to-end packet delays.

VII. Conclusion

This work highlights the importance of multi-homing support in the integrated heterogeneous wireless networks of 3GPP and non-3GPP access technologies. The existing 3GPP specifications for integration of two types of the access technologies are extended following IETF standards to realize multi-homing support for the users. Following the proposed extensions, a network simulation model is developed, where 4G LTE and WLAN co-exist. This work also focuses on the problem of optimum resource utilization in such a heterogeneous network where the users and network operators can take advantage of multi-homing support. The problem of optimum network resource allocation is mathematically modeled using the linear programming technique. The proof of concept is provided through the simulation results. With help of simulation results it is shown that the proposed scheme of resource allocation brings twofold gain when compared to the 3GPP proposal. On the one hand, it significantly improves the network capacity and on the other hand it fulfills the user application QoS demands, which otherwise cannot be satisfied from QoS unaware non-3GPP access technologies.

VIII. Acknowledgment

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7) under grant agreement no. 257448.

References

[1] 3GPP Technical Report TS 25.814, Physical layer aspects for E-UTRA, 3rd Generation Partnership Project, v.7.1.0, Sept. 2006

[2] Q. Song and A. Jamalipour, Network Selection in an Integrated Wireless LAN and UMTS Environment using Mathematical Modeling and Computing Techniques, IEEE Wireless Commun., June 2005

[3] W. Song, H. Jiang, and W. Zhuang, Performance analysis of the WLAN-first scheme in cellular/WLAN interworking, IEEE Trans. Wireless Commun., vol. 6, May 2007

[4] W. Song, H. Jiang, and W. Zhuang, "Call admission control for integrated voice/data services in cellular/WLAN interworking", IEEE ICC06, vol. 12, June 2006.

[5] F. Yu, V. Krishnamurthy, Optimal Joint Session Admission Control in Integrated WLAN and CDMA Cellular Networks with Vertical Handoff, IEEE transaction on Mobile Computing, vol. 6, Jan. 2007

[6] H. Zhai, X. Chen, Y. Fang, How Well Can the IEEE 802.11 Wireless LAN Support Quality of Service?, IEEE Trans. Wireless Commun., vol. 4, 2005

[7] S. Lincke-Salecket, Load shared integrated networks, Personal Mobile Communications Conference, 2003

[8] Y. Zaki, T. Weerawardane, C. Görg and A. Timm-Giel, Multi-QoS-Aware Fair Scheduling for LTE, VTC Spring, 2011

[9] U., Toseef, Y., Zaki, A., Timm-Giel, C., Grg., Development of Simulation Environment for Multi-homed Devices in Integrated 3GPP and non-3GPP Networks, The 10th MobiWAC conference, Paphos, 2012

[10] 3GPP Technical Report TS 36.213, Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures, v10.2.0, June 2011

[11] J. Klaue, B. Rathke, and A. Wolisz, EvalVid - A Framework for Video Transmission and Quality Evaluation, 13th International Conference on Modeling Techniques and Tools for Computer Performance Evaluation, pp. 255-272, Illinois, USA, Sept. 2003.

[12] U. Toseef, M. Li, A. Balazs, X. Li, A. Timm-Giel, C. Görg, Investigating the Impacts of IP Transport Impairments on VoIP service in LTE Networks, 16th VDE/ITG Fachtagung Mobilkommunikation, 2011

[13] 3GPP Technical Report TS 23.402, Architecture enhancements for non-3GPP accesses, 3rd Generation Partnership Project, v10.6.0, Dec. 2011.

[14] OPNET website, http://www.opnet.com, as accessed in Sept. 2012

[15] IBM CPLEX Optimizer, http://www.ibm.com, as accessed in Sept. 2012

[16] G. Bianchi, Performance Analysis of the IEEE 802.11 Distributed Coordination Function, IEEE Journal on Selected Areas in Communications, Vol. 18, No. 3, pp. 535-547, Mar. 2000.

[17] R. Litjens, F. Roijers, J. L. van den Berg, R. J. Boucherie,and M. Fleuren, Performance Analysis of wireless LANs: an Integrated Packet/Flow Level Approach, ITC Conference, Berlin, Germany, Aug. 2003.

 ISBN: 978-1-61208-231-8

Optimal Network Selection for Mobile Multicast Groups

Svetlana Boudko and Wolfgang Leister
Norsk Regnesentral, Oslo, Norway
Email: {svetlana.boudko, wolfgang.leister}@nr.no

Stein Gjessing
University of Oslo, Norway
Email: steing@ifi.uio.no

***Abstract*—Mobile devices are typically equipped with multiple access network interfaces, supporting the coexistence of heterogeneous wireless access networks. The selection of an optimal set of serving mobile networks for multicast streams is a challenging problem. We consider a network selection problem for multicast groups of mobile clients that operate in a heterogeneous wireless access network environment. We present a solution to this problem with an optimal allocation of mobile users to multicast groups when multiple mobile networks are available for operation. This solution is suited for small scale networks and can be used as reference for complex networks.**

***Index Terms*—Wireless networking, mobile network selection, decentralized algorithms.**

I. Introduction

The increasing market of mobile devices and mobile services, continuous development and diversification of user terminals as well as availability of various wireless network technologies challenge resource limitations of wireless access networks. This requires consideration of the resource allocation problem from the different angle, including collaboration between mobile users and networks in improvement of the utilization of resources. Referring to wireless access networks, the ability to be connected to several network technologies poses new challenges in formulating effective strategies for selecting the best network. The network selection problem inspired by the "always best connected" concept was mostly focused on the definition of metrics to address the end user quality of service and considered the problem from a single user view point.

Multicast [1] is an efficient method for point-to-multipoint communications, which reduces drastically the usage of network resources when the same content is sent to a large group of users. Different types of applications like video conferencing, file distribution, live multimedia streaming can benefit from deploying multicast networking. However, the well-known complexity of managing multicast networks makes the deployment of multicast even more challenging in wireless environments when mobility issues have to be considered. In this paper, we consider a solution for the network selection problem for heterogeneous mobile networking as a part of multicast group management.

The remainder of the paper is organized as follows. After presenting an overview of related work in Section II, we discuss a representative scenario in Section III. We present the problem formulation and outline a suitable algorithm in Section IV. A usage example and test results are given in Section V, before discussing future work and concluding in Section VI and Section VII, respectively.

II. Related Work

To the best of our knowledge, the research field concerning selection of a network in heterogeneous wireless networks from a perspective of multicast delivery is not well exploited. Most previous works for mobile multicast focus on optimal multicast tree construction in multihop ad hoc networks [2–5].

Ormond and Murphy [6] propose a network selection approach that uses a number of possible utility functions. This solution is user-centric, and an interplay between different users and networks is not considered; neither is a multicast scenario. Ormond and Murphy conclude that the impact of multiple users operating in the same region needs to be further examined.

Gluhak et al. [7] consider the problem of selecting the optimal bearer paths for multicast services with groups of heterogeneous receivers. The proposed algorithm selects the bearer path based on different optimization goals. However, Gluhak et al. address the problem only for the ideal static multicast case without taking into account users crossing different cells. In their work, multicast membership does not change during the duration of a service, and multicast groups are not built with consideration of users' movements. In our opinion, this is not a realistic case for wireless networks.

Yang and Chen [8] propose a bandwidth-efficient multicast algorithm for heterogeneous wireless networks that is formulated as an Integer Linear Programming problem that is solved using Lagrangian relaxation [9]. The algorithm deals only with constructing optimal shortest path trees for multicast groups. In this approach, important parameters such as cost of service, user's velocity, etc. are not considered.

Jang et al. [10] present a mechanism for efficient network resource usage in a mobile multicast scenario. This mechanism is developed for heterogeneous networks and implements network selection based on network and terminal characteristics and Quality of Service (QoS). However, in the proposed mechanism, the network selection is performed purely based on terminal's preferences, the network perspective is not considered, and the solution does not optimize the utilization of network resources.

 ISBN: 978-1-61208-231-8

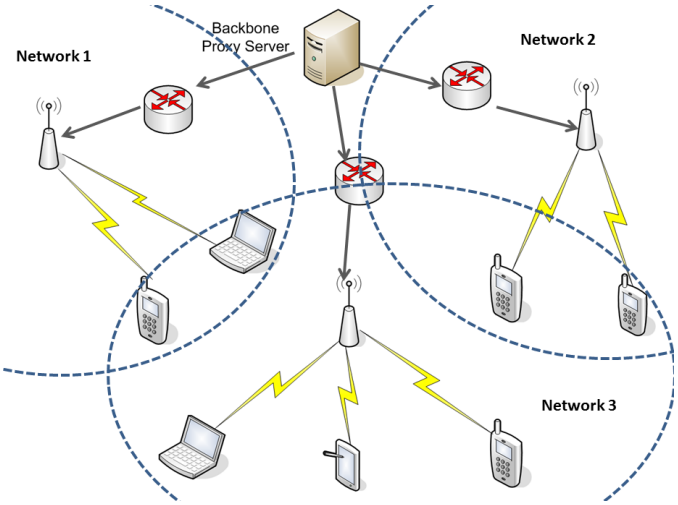


Figure 1. Multicast streaming scenario for a group of mobile clients served by several mobile networks before regrouping.

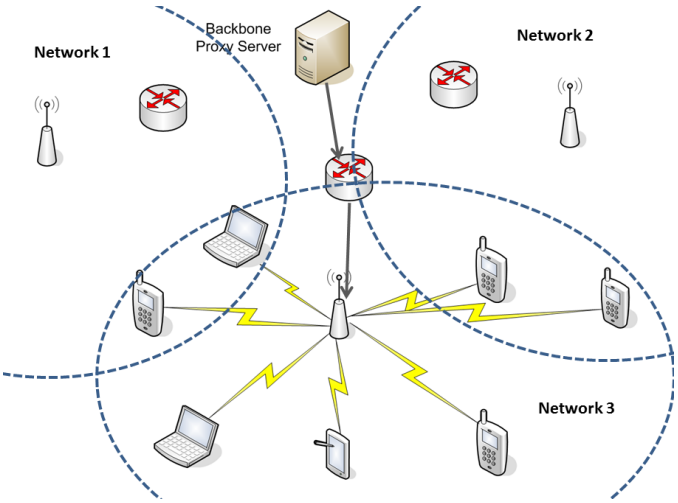


Figure 2. Multicast streaming scenario for a group of mobile clients switched to one mobile network after regrouping.

In our analysis, we recognize that the presented previous work has not addressed several important aspects related to the network selection for mobile multicast groups. We need to study how the users' movements influence the optimal selection of members for multicast groups and how the information needed for network selection is exchanged between the decision makers.

III. Scenario

To illustrate the yet unsolved challenges for optimal network selection in multicast networks, we consider a multimedia streaming scenario for a group of mobile users that concurrently receive the same content from the Internet. We assume that a backbone proxy server (BPS) is placed at the network edge. The BPS is a member of a content distribution system (CDN). This scenario is an extension of a scenario that we previously have considered to illustrate an adaptive multimedia streaming architecture to mobile nodes [11].

The BPS streams content that either is hosted on the server, or resends the streaming content as a part of an application layer multicast. The users of this network are located in an area with a substantial overlap in coverage of several mobile networks, and are connected to different networks. The base stations of the system have multicast capabilities, implementing, for example, Multimedia Broadcast Multicast Service [12]. A representative scenario of such networking is illustrated in Figure 1.

In our scenario, the mobile terminals are capable to connect to several access networks, and vertical handoffs between these networks are technically possible. Further, we assume that these terminals are equipped with GPS receivers, so that their location information can be transmitted to the BPS. The BPS can use this information to determine how the users can be regrouped in multicast groups. Such regrouping is beneficial as it saves network resources. Hence, the users that get the same content can exploit the same wireless link because the content can be broadcasted to them. The resources in the backhaul network are also better utilized because the content is now delivered only to one mobile network instead of being spread to several networks. An example of such regrouping is depicted in Figure 2.

Technically, to facilitate such a mechanism, the user terminals will have the possibility to switch to other mobile networks after receiving certain messages from the BPS. Since users may have different preferences depending on diverse criteria, for example, power consumption, security, network cost of service, etc., the interplay between the users' utilities and the networks' utilities is important to consider. In the current paper, we formulate and solve the problem, which solution gives us an optimal allocation of mobile users to mobile networks.

IV. Problem Formulation

In this section, we formalize the scenario discussed in Section III.

We consider a set of networks $N = 1, 2, \ldots, n$, a set of mobile nodes $M = 1, 2, \ldots, m$ and a set of streaming contents $S = 1, 2, \ldots, s$. Each content s_k can be delivered to more than one mobile node m_j. Therefore, using multicast for data dissemination is beneficial. For each node m_j and network n_i, the following is defined: available bandwidths of networks are denoted by b_i; streaming bitrate requirements of mobile nodes that request content s_k are denoted by r_k; $rss_{i,j}$ is the received signal strength in network n_i for terminal m_j, while power consumption and the cost of service in network n_i for node m_j are denoted by $p_{i,j}$ and $c_{i,j}$, respectively.

For each node m_j, we define a user preference profile that is described by a tuple containing Th_j^p, Th_j^c, and Th_j^{rss}. These denote thresholds or user preferences, for, respectively, power consumption, cost of service and received signal strength.

For each node m_j and each mobile network n_i we define

 ISBN: 978-1-61208-231-8

an availability function δ as follows:

$$\delta(i,j) = \begin{cases} 1, \text{if } n_i \text{ is available for } m_j \\ 0, \text{if not} \end{cases} \quad (1)$$

For each mobile network n_i and each streaming content s_k we define a function γ as follows:

$$\gamma(i,k) = \begin{cases} 1, \text{if at least one } m_j \text{ receives } s_k \text{ in } n_i \\ 0, \text{if not} \end{cases} \quad (2)$$

We define a decision variable $x_{i,j}$ as follows:

$$x(i,j) = \begin{cases} 1, \text{if } n_i \text{ is assigned for } m_j \\ 0, \text{if not} \end{cases} \quad (3)$$

To find the best possible allocation of the mobile nodes to the available networks in terms of minimization of consumed bandwidth, we minimize the following objective function:

$$\min \sum_{n_i \in N} \sum_{s_k \in S} \gamma(i,k) \cdot r_k \quad (4)$$

The objective function is subject to the set of constraints given below.

We need to garantee that each mobile node is assigned to one network.

$$\forall\{i\} : \sum_j \delta_{i,j} \cdot x_{i,j} = 1 \quad (5)$$

We need to specify that user preferences defined in their profiles are satisfied.

$$\forall\{i,j\} : x_{i,j} \cdot p_{i,j} \leq Th_j^p \quad (6)$$

$$\forall\{i,j\} : x_{i,j} \cdot c_{i,j} \leq Th_j^c \quad (7)$$

$$\forall\{i,j\} : x_{i,j} \cdot rss_{i,j} \geq Th^r ss_j \quad (8)$$

The defined problem is a typical integer linear programming problem. To solve this problem we have taken advantage of the MATLAB Optimization Toolbox. We use the function *bintprog*, which solves problems of the following form

$$\min_x f^T x \text{ such that } \begin{cases} \mathbf{A} \cdot x \leq b, \\ \mathbf{A_{eq}} \cdot x = b_{\text{eq}}, \\ x \text{ binary.} \end{cases} \quad (9)$$

V. Usage Example

The system computes the optimal assignment of mobile nodes to networks for a given static network condition and application situation. It is not a topic of this paper to compare any existing network selection algorithms with this system, but we consider it necessary to demonstrate that the optimal network selection decision does not have a trivial solution in the general case. We have done this by applying the computation to several network topologies. Here, we show the examples.

Table I
Total consumed bandwidth of the system.

Number of networks	Random	Optimum
4	26144	8072
5	32680	7560
6	39216	6536

We consider a scenario with four, five and six wireless networks and 1000 mobile users in the system. Not all of these networks are simultaneously available for all users. We consider two local WLANs that do not cover the whole area in consideration and, therefore, not all users have the access to these networks. 25% of users can access both WLANs, 50% can access one of them *equally distributed*, and 25% can access none of the WLANs. The rest of the networks deploy 4G LTE technology. Further, we divide the requested content into four categories in terms of required bandwidth, 512 kbps, 1024 kbps, 2000 kbps, and 3000 kbps.

In this experiment, we evaluate the total consumed bandwidth for all networks. The results for the total bandwidth in kbps are shown in Table I. We see clearly that the system achieves a much higher throughput than the random network selection approach.

VI. Discussion

The implementation of the algorithm in real systems requires that all knowledge of network resources and preference profiles of users is available to the BPS or some other central unit that decides upon how the data transmission shall be constructed. This implies that a significant number of messages needs to be exchanged inside the system, which comes at the cost of increased delays, need for network resources, and computation resources on mobile devices. To overcome this problem, we need an algorithm that is designed to handle the aforementioned information uncertainty. Several research studies address combinatorial problems that contain input data, which cannot be obtained accurately [13–15]. The problem discussed in Section IV will be reformulated using the results of these studies. This requires that the thresholds in the constraints 6, 7, and 8 are replaced with probabilities for these preferences.

VII. Conclusion

The paper studied the problem of selecting the optimal network for multicast groups of mobile clients in multi-stream scenario based on mobile clients' preferences and location information. We proposed a method that provides the optimal assignment for a given network topology, network conditions and user preferences.

Since the calculation is rather computing-intensive, and since the knowledge of the entire system state is necessary for the calculation, we conclude that this method is not suited for large scale networks due to scalability reasons. However, the method can be used for small scale networks and, mostly important, we intend to use the method as a reference to evaluate related algorithms that allow network selection in

 ISBN: 978-1-61208-231-8

a decentralized manner with only limited information shared among the decision makers.

As a further step, we intend to develop distributed algorithms that operate under partial knowledge of the network topology and conditions, inaccurate knowledge of clients' preferences, dynamically changing networking parameters such as available bandwidth of mobile networks and network availability for mobile nodes.

VIII. Acknowledgment

The work described in this paper has been conducted as a part of the ADIMUS (Adaptive Internet Multimedia Streaming) project, which is funded by the NORDUnet-3 programme.

References

[1] K. Savetz, N. Randall, and Y. Lepage, *MBONE: Multicasting Tomorrow's Internet*, 1st ed. Foster City, CA, USA: IDG Books Worldwide, Inc., 1995.

[2] M. Gerla, C.-C. Chiang, and L. Zhang, "Tree multicast strategies in mobile, multishop wireless networks," *Mob. Netw. Appl.*, vol. 4, no. 3, pp. 193–207, Oct. 1999.

[3] C.-C. Chiang, M. Gerla, and L. Zhang, "Forwarding group multicast protocol (FGMP) for multihop, mobile wireless networks," *Cluster Computing*, vol. 1, no. 2, pp. 187–196, Apr. 1998.

[4] J. G. Jetcheva, "Adaptive demand-driven multicast routing in multi-hop wireless ad hoc networks," Ph.D. dissertation, Carnegie Mellon University, Pittsburgh, PA, USA, 2004.

[5] J. Yuan, Z. Li, W. Yu, and B. Li, "A cross-layer optimization framework for multihop multicast in wireless mesh networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 11, pp. 2092 –2103, nov. 2006.

[6] O. Ormond and J. Murphy, "Utility-based intelligent network selection," in *IEEE Int'l Conf. on Communications, ICC*, 2006.

[7] A. Gluhak, K. Chew, K. Moessner, and R. Tafazolli, "Multicast bearer selection in heterogeneous wireless networks," in *IEEE Int'l Conf. on Communications, ICC*, vol. 2, May 2005, pp. 1372–1377.

[8] D.-N. Yang and M.-S. Chen, "Efficient resource allocation for wireless multicast," *IEEE Transactions on Mobile Computing*, vol. 7, no. 4, pp. 387–400, Apr. 2008.

[9] M. L. Fisher, "The lagrangian relaxation method for solving integer programming problems," *Manage. Sci.*, vol. 50, no. 12 Supplement, pp. 1861–1871, Dec. 2004.

[10] I.-S. Jang, W.-T. Kim, J.-M. Park, and Y.-J. Park, "Mobile multicast mechanism based mih for efficient network resource usage in heterogeneous networks," in *Proc. of the 12th Int'l Conf. on Advanced Communication Technology*, ser. ICACT'10, 2010, pp. 850–854.

[11] W. Leister, T. Sutinen, S. Boudko, I. Marsh, C. Griwodz, and P. Halvorsen, "An architecture for adaptive multimedia streaming to mobile nodes," in *MoMM '08: Proc. 6th Int'l Conf. on Advances in Mobile Computing and Multimedia*. ACM, 2008, pp. 313–316.

[12] G. Xylomenos, V. Vogkas, and G. Thanos, "The multimedia broadcast/multicast service," *Wireless Communications and Mobile Computing*, vol. 8, no. 2, pp. 255–265, 2008.

[13] G. B. Dantzig, "Linear programming under uncertainty," *Manage. Sci.*, vol. 50, no. 12 Supplement, pp. 1764–1769, Dec. 2004.

[14] J. R. Birge and F. Louveaux, *Introduction to Stochastic Programming*, ser. Springer Series in Operations Research and Financial Engineering. Springer, 1997.

[15] D. J. Bertsimas, P. Jaillet, and A. R. Odoni, "A priori optimization," *Oper. Res.*, vol. 38, no. 6, pp. 1019–1033, Jan. 1991.

 ISBN: 978-1-61208-231-8

CobCel: Distributed and Collaborative Sensing of Cellular Phone Coverage Using Google Android

Jonathan Pino and Jorge E. Pezoa
Electrical Engineering Department and The Center for Optics and Photonics
Universidad de Concepción, Concepción, Chile
Email: {jonpino,jpezoa}@udec.cl

***Abstract*—This paper presents CobCel, a prototype Android application for measuring, in a distributed and collaborative manner, the cellular coverage as perceived by the users of mobile devices. Unlike specialized cellular coverage tests, CobCel samples the received signal strength indication (RSSI) using smartphones operated by their own users. The sensed RSSI is supplied with the geographical location of the device, and this supplemented information is next transmitted to a server which aggregates the collaboratively sensed data and displays a historical cellular coverage map as perceived by the cellphone users. Data collected by CobCel is intended to be used not only to report cellular coverage, but also to create open-source databases of cellular coverage and end-users mobility patterns. Further, it has been noticed after analyzing the data that real-world RSSI samples seems to follow a heavy-tail law instead of the chi-squared distribution usually assumed in theory.**

***Keywords*-Distributed Sensing; RSSI; Collaborative Sensing; Google Android**

I. INTRODUCTION

Cellular networks are nowadays extensively used to provide voice and data services. The major concern of cellular service providers is supplying a high quality service to their customers. The aforementioned quality-of-service is primarily assessed by measuring cellular network coverage using standard tests and specialized equipment [1]. Lately, customers, which are always concerned about obtaining the quality-of-service they are paying for, have taken the matter (literally) in their own hands and exploited the capabilities of modern smartphones to conduct their own assessment of the cellular coverage. Examples of such efforts are the website CellReception [2] and applications like Sensorly and OpenSignalMaps [3], [4].

CobCel is yet another application for collaboratively measuring the cellular coverage of cellphone systems. CobCel is a prototype Android application that differs from specialized cellular coverage tests in several ways. First, specialized test use expensive equipment to take samples of the received signal strength indication (RSSI) [5] CobCel instead uses inexpensive smartphones as sensors. Second, specialized test take data on the streets from a moving or fixed vehicle [5], while CobCel collects samples of the RSSI not only on the streets, but also at any location a user of a mobile phone may visit during the day such as buildings, elevators, shopping malls, etc. Third, during drive-tests, antennas are usually either outside of the vehicle or inside of the vehicle at a place where occlusions can be reduced [5]. CobCel is an end-user application which no requires special attention from the user, hence, samples of the RSSI are typically taken from users' pockets, bags, purses, etc. Lastly, drive tests normally conduct measurements using pre-established routes and places [5]. Since CobCel takes samples from several users at any time in a collaborative manner, the geographical and temporal diversity achieved by the samples of the RSSI is large, thereby creating a well-representative data pool of the cellphone coverage. Because of this geographical and temporal diversity, data collected by means of CobCel is intended to be used not only to assess and report cellular coverage, but also to create an open-source database of cellular coverage and end-users mobility patterns.

This paper is organized as follows. In Section II, we present related work on the subject. In Section III, we describe the design of the CobCel application. Section IV presents results. Our conclusions are given in Section V.

II. RELATED WORK

Among all the applications available to measure the cellular coverage, Sensorly [3], and OpenSignalMaps [4] are the most popular. These applications are of special interest to this work because they serve the same purpose as CobCel. Sensorly is an Android-based application and a website aiming to help cellular phone operators to improve their network quality [3]. Sensorly collects, processes, and displays end-user supplied measurements of the signal quality of 4G [6], CDMA [7], GSM [7], and WiFi [8] networks from all over the world, thereby providing "a unique perspective on network experience as perceived by real life users" [3]. Sensorly provides to its users free maps on both the Android Market and the Internet. Unlike CobCel, Sensorly provides as well information on the network speed, the cause of dropped calls, and means to compare different service providers. Similarly, the software OpenSignalMaps, developed by Staircase 3 Inc., has built a database of cell phone towers, cell phone RSSI, and Wi-Fi access points from all over the world. Data is sensed collectively by the end-users running OpenSignalMaps' Android application [4]. As in

 ISBN: 978-1-61208-231-8

the case of Sensorly, OpenSignalMaps shows at its website the collected data and plots also heat maps exhibiting the strength of the received signal at any particular area. Some of the unique features of OpenSignalMaps are the display of the signal direction and the display of radar views of cell towers and Wi-Fi routers. It must be commented that both applications, Sensorly and OpenSignalMaps, take care of privacy issues, and aim to save processing power and battery. CobCel differs from any other application is that the data collected is intended to be used not only to assess and report cellular coverage, but also to create an open-source database of cellular coverage and end-users mobility patterns.

III. Application Design

Overview. CobCel exploits the standard functions supplied by Google Android to read cellphone's RSSI. In addition, and to provide a fairly accurate geographical location for the measurements, GPS information is also collected. Once the RSSI is sensed, a fixed-size data packet, which contains additional information such as time, local area code (LAC), and mobile network code (MNC), is created and transmitted to a server which aggregates the sensed data and displays a historical cellular coverage map as perceived by the cellphone users. CobCel and its associated visualization system is an open-source effort which exploits both Google's software tools and MySQL [9] to yield a distributed sensing platform which allows to measure and display the RSSI at any geographical location. Figure 1(a) depicts the overview of the CobCel and its storage and display platform.

Requirements. In developing CobCel, the following requirements have been considered: (i) the operating system must be Android 2.2 for compatibility; (ii) a GPS locator must be available to accurately locate the RSSI samples; (iii) the smartphone must be able to query the LAC, the MNC, and the cellular tower ID, to properly store and display cellular network information; (iv) the use of CPU, storage, and batteries must be scarce; and (v) the anonymity of the sensed data must be guaranteed. The last requirement is achieved by never storing or sending smartphone's sensible information such as the international mobile equipment identity (IMEI). Also, the user must be capable of adjusting the following parameters: the minimum time between consecutive samples, the minimum distance between consecutive samples, and enabling/disabling the energy savings policy (ESP).

Battery savings. The following means have been provided in CobCel to save batteries. First, the type of communication to be used by the smartphone prior to transfer the sensed data. According to [10], a Wi-Fi connection consumes less power than a cellular data connection; we have prioritized the use of a Wi-Fi connection over cellular data. Second, due to the sensed data is not time-sensitive, an ESP that delays the transmission of the sensed data until the smartphone is connected to a Wi-Fi network has been

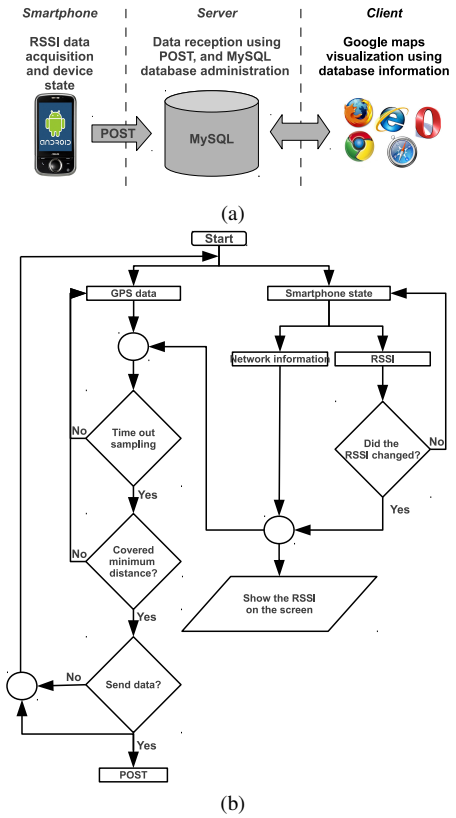


Figure 1: (a) Overview of the CobCel application and its storage and display platform. (b) CobCel's flow diagram.

implemented. Third, and also to provide the user a means to adjust the amount of data to be sensed and transmitted, we have included in CobCel parameters for selecting the sampling time and distance of the application.

Application's state definition. According to the modes of operation of a smartphone, the battery savings policy, and the application requirements, the following states have been defined for the CobCel application. *State 1:* the smartphone has cellular coverage, data service, and the ESP is disabled. *State 2:* the smartphone has cellular coverage, data service, and the ESP is enabled. *State 3:* the smartphone has cellular coverage yet no data service, and the ESP is either enabled or disabled. *State 4:* the smartphone has no cellular coverage. *State 5:* the smartphone is in airplane mode or any other mode where RSSI cannot be sampled.

All the aforementioned application states and requirements, as well as the energy constraints, have been considered in the design of CobCel's work flow, which has depicted in Fig. 1(b). The most relevant steps in the application work flow are detailed next. Once the application is executed the state of the smartphone is determined. If the smartphone is in state 1, 2, or 3, the RSSI is sampled using the function `getSystemService()`. Clearly, for the other two states, the RSSI cannot be retrieved. Simultaneously, and if the smartphone is in state 1, 2, or 3,

 ISBN: 978-1-61208-231-8

the geographical location of the device is acquired using Android's class `LocationListener` and the function `requestLocationUpdates()`. Next, if the RSSI was sampled, CobCel checks if both the minimum time and the minimum distance criterion between consecutive samples has been fulfilled to store the sampled RSSI value. Finally, CobCel checks if the ESP is disabled, and if it does, it sends the data prioritizing the use of a Wi-Fi connection over a cellular data service. Otherwise, CobCel follows the ESP and delays the transmission of the sensed RSSI data until the smartphone is connected to a Wi-Fi network.

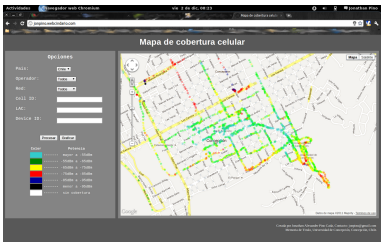
IV. Results

The CobCel application is available at the Google Play store [11]. To date, the application has been installed more than 5,000 times and data from several countries has been collected in our database. Figure 2(a) shows a sample map of the cellphone coverage in Concepción, Chile. We comment that date and time information are also transmitted with the RSSI and geographical position samples. Thus, we note that, with this spatial and temporal information, we may indeed use CobCel's sampled data to generate an open-source database of actual end-used mobility. As an example of this added feature, we comment that the map in Fig. 2(a) does correspond to a sample mobility test of an Android user in downtown Concepción.

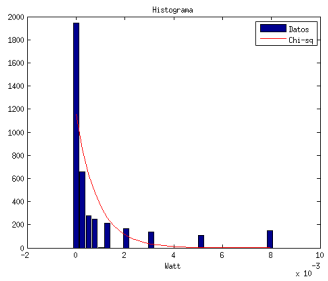
Lastly and to show the potential of CobCel in generating an open-source database of cellular coverage, we fitted an empirical distribution for the RSSI and compared it to its theoretical distribution. According to most theoreticians, the RSSI in open areas follows closely a chi-squared distribution [7]. The fitted and theoretical distribution for the RSSI are shown in Fig. 2(b). The fitted distribution was constructed by pooling data from several users connected to the same cellular tower, and due to the non-Gaussian nature of the data, we employed Doane's formula to determine the number of data bins. From Fig. 2(b) we conclude that real-world data seems to follow a heavy-tail law instead of a chi-squared.

V. Conclusion and Future Works

We presented CobCel, a prototype application for measuring, in a distributed and collaborative manner, the cellular coverage as perceived by the users of mobile devices. By sampling the RSSI and the geographical location of a mobile device, historical maps of cellular coverage can be displayed allowing the users to assess the service supplied by different service providers. Data collected by CobCel is intended to be used not only to report and assess cellular coverage, but also to create open-source databases of cellular coverage and end-users mobility patterns. The application is available for testing at Google Play and appears to be a useful tool for creating open-source databases of cellular coverage and end-users mobility patterns.



(a)



(b)

Figure 2: (a) Sample map of the cellphone coverage in Concepción, Chile. (b) Fitted and theoretical RSSI curves.

As a future work, we will merge the RSSI measurements with speed, reliability, and availability measurements and we will conduct surveys with the goal of measure the quality of experience of the users in regards to their service providers.

Acknowledgment

The authors acknowledge the support of Fondecyt Project 11110078 and Basal Project FB024.

References

[1] I. Kostanic, N. Mijatovic, and S. Vest, "Measurement based qos comparison of cellular communication networks," in *IEEE Int. Workshop on Com. Quality & Reliability*, 2009.

[2] Mobiledia, "Cell reception," Internet: http://www.cellreception.com/, 2002, [Online; retrieved: September 2012].

[3] Sensorly, "Coverage Maps Sensorly," Internet: http://www.sensorly.com/, 2011, [Online; retrieved: September 2012].

[4] Staircase 3 Inc., "OpenSignalMaps - Cell Phone Tower and Signal Heat Maps," Internet: http://opensignalmaps.com/,, 2012, [Online; retrieved: September 2012].

[5] W. Lee, *Mobile Communications Eng.* McGraw-Hill, 1982.

[6] E. Dahlman, S. Parkvall, and J. Skold, *4G: LTE/LTE-Advanced for Mobile Broadband.* Academic Press, 2011.

[7] D. Tse and P. Viswanath, *Fundamentals of Wireless Communications*. Cambridge University Press, 2005.

[8] C. Smith and J. Meyer, *3G Wireless with 802.16 and 802.11: WiMAX and WiFi.* McGraw-Hill, 2011.

[9] Oracle, "MySQL," Internet: http://www.mysql.com, 2012, [Online; retrieved: September 2012].

[10] Google Inc., "Coding for Life–Battery Life, That Is," Internet: http://www.google.com/events/io/2009/sessions/CodingLifeBatteryLife.html, 2009, [Online; retrieved: September 2012].

[11] J. Pino and J. E. Pezoa, "CobCel: Cobertura Celular," Internet: https://play.google.com/store/apps/details?id=itux.cobertura.cl, 2012, [Online; retrieved: September 2012].

 ISBN: 978-1-61208-231-8